Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 29, 2017

M. Boucadair
Orange
T. Reddy
McAfee
P. Patil
Cisco

June 27, 2017

Distributed-Denial-of-Service Open Threat Signaling (DOTS) Server Discovery
draft-boucadair-dots-server-discovery-00

Abstract

It may not be possible for a network to determine the cause for an attack, but instead just realize that some resources seem to be under attack. To fill that gap, Distributed-Denial-of-Service Open Threat Signaling (DOTS) allows a network to inform a server that it is under a potential attack so that appropriate mitigation actions are undertaken.

This document specifies mechanisms to configure nodes with DOTS servers.

Table of Contents

1. Introduction

In many deployments, it may not be possible for a network to determine the cause for a distributed Denial-of-Service (DoS) attack [RFC4732], but instead just realize that some resources seem to be under attack. To fill that gap, the IETF is specifying an architecture, called DDoS Open Threat Signaling (DOTS) [I-D.ietf-dots-architecture], in which a DOTS client can inform a DOTS server that the network is under a potential attack and that appropriate mitigation actions are required. Indeed, because the lack of a common method to coordinate a real-time response among involved actors and network domains inhibits the effectiveness of DDoS attack mitigation, DOTS protocol is meant to carry requests for DDoS attack mitigation, thereby reducing the impact of an attack and leading to more efficient defensive actions.
[I-D.ietf-dots-use-cases] identifies a set of scenarios for DOTS; almost all these scenarios involve a CPE.

The basic high-level DOTS architecture is illustrated in Figure 1 ([I-D.ietf-dots-architecture]):

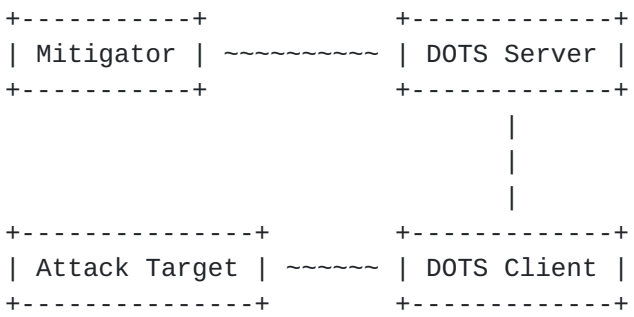


Figure 1: Basic DOTS Architecture

[I-D.ietf-dots-architecture] specifies that the DOTS client may be provided with a list of DOTS servers; each associated with one or more IP addresses. These addresses may or may not be of the same address family. The DOTS client establishes one or more signaling sessions by connecting to the provided DOTS server addresses. The logic for connecting to one or multiple IP addresses is out of scope of this document.

This document specifies methods for DOTS clients to discover their DOTS server(s). The rationale for specifying multiple discovery mechanisms is discussed in Section 4.

Considerations for the selection of DOTS server(s) by multi-homed DOTS client is out of scope; the reader should refer to [I-D.boucadair-dots-multihoming] for more details.

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

This document makes use of the following terms:

- DDoS: A distributed Denial-of-Service attack, in which traffic originating from multiple sources are directed at a target on a network. DDoS attacks are intended to cause a negative impact on the availability of servers, services, applications, and/or other functionality of an attack target.
- DHCP refers to both DHCPv4 [RFC2131] and DHCPv6 [RFC3315].
- DHCP client denotes a node that initiates requests to obtain configuration parameters from one or more DHCP servers.
- DHCP server refers to a node that responds to requests from DHCP clients.
- DOTS client: A DOTS-aware software module responsible for requesting attack response coordination with other DOTS-aware elements.
- DOTS server: A DOTS-aware software module handling and responding to messages from DOTS clients. The DOTS server should enable mitigation on behalf of the DOTS client, if requested, by communicating the DOTS client's request to the mitigator and returning selected mitigator feedback to the requesting DOTS client. A DOTS server may also be a mitigator.
- DOTS gateway: A DOTS-aware software module that is logically equivalent to a DOTS client back-to-back with a DOTS server.

The reader should be familiar with other terms defined in [I-D.ietf-dots-architecture] and [RFC3958].

4. Why Multiple Discovery Mechanisms?

It is tempting to specify one single discovery mechanism for DOTS. Nevertheless, the analysis of the various use cases sketched in [I-D.ietf-dots-use-cases] reveals that it is unlikely that one single discovery method can be suitable for all the sample deployments (Table 1). Concretely:

- Almost all the use cases do involve a CPE device. Multiple CPEs, connected to distinct network providers may even be considered. It is intuitive to leverage on existing mechanisms such as DHCP to provision the CPE acting as a DOTS client with the DOTS server(s). Further, the use of a dedicated DHCP option is used as an explicit signal to activate the DOTS service.

- The upstream network provider is not the DDoS mitigation provider for some of these use cases. The use of anycast is not appropriate for this use case, in particular. It is safe to assume that for such deployments, the DOTS server(s) domain name is provided during the service subscription (i.e., configuration file).

- Multiple DOTS clients may be enabled within a network (e.g., enterprise network). Automatic means to discover DOTS servers in a deterministic manner are interesting from an operational standpoint.

- Some of the use cases may involve a DOTS gateway that is responsible for forking requests received from internal DOTS clients to upstream DOTS servers or for selecting the appropriate DOTS server. Particularly, the use of anycast may simplify the operations within the enterprise network to discover a DOTS gateway, if the enterprise network is single-homed.

- Some of the use cases may allow DOTS clients to have direct communications with upstream DOTS servers; that is no DOTS gateway is involved. Leveraging on existing features that do not require specific feature on the node embedding the DOTS client may ease DOTS deployment. Typically, the use of Straightforward-Naming Authority Pointer (S-NAPTR) lookups [RFC3958] together with existing DHCP options is an interesting technique to achieve DOTS server discovery.

- Resolving a DOTS server domain name provisioned to a DOTS client into IP address(es) require the use of the appropriate DNS resolvers; otherwise, resolving those names will fail. The use of protocols such as DHCP does allow to associate provisioned DOTS server domain names with a list of DNS servers to be used for name resolution.

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
Enterprise with an upstream transit provider DDoS mitigation Service	Yes	Yes
Enterprise with a Cloud DDoS Mitigation Provider	Yes	No
Homenet DDoS Detection Collaboration for ISP network management	Yes	Yes
DDoS Orchestration	No	N/A

Table 1: Summary of DOTS Use Cases

Consequently:

- This document specifies DHCP options that can be used to configure nodes, embedding a DOTS client, with DOTS servers' names (Section 6). These names will be resolved into one or a list of IP addresses. The use of DHCP for DOTS provisioning is justified because many of the target use cases identified in [I-D.ietf-dots-use-cases] involve CPEs; these devices widely support DHCP. Also, the use of DHCP to provision a name that will be resolved into one or many IP address(es) of the appropriate DOTS server(s) to contact, does not suffer from the complications encountered if a anycast address is used (see Section 3.2.4.1 of [I-D.ietf-dots-architecture]). Further, the use of DHCP ensures a deterministic behavior since DHCP can also be used to provision a list of DNS servers that can be used to resolve DOTS server domain names.

- Also, the document specifies how S-NAPTR can be used for dynamic DOTS server discovery (Section 7).

- Last, the document reserves IP anycast addresses for DOTS usage (Section 9).

A common logic to build the DOTS servers list is elaborated in Section 5.

5. How to Build the List of DOTS Servers?

In order to encourage consistent DOTS behaviors while allowing for automated DOTS server discovery, the following procedure MUST be followed by a DOTS client to built a DOTS server(s) list to contact:

1. if the DOTS client is explicitly configured with DOTS servers (e.g., local configuration file, DHCP), that list of DOTS servers is used, else

2. if DOTS service name(s) are configured, those names are used to retrieve the corresponding DOTS servers list, else

3. the DOTS client uses the DOTS anycast addresses (IPv4/IPv6) to contact it DOTS server(s).

The above procedure MUST also be followed by a DOTS gateway.

Details specific to each aforementioned step are elaborated in Sections 6,7, and 9.

6. DHCP Options for DOTS

6.1. Design Rationale

As reported in Section 1.7.2 of [RFC6125], "few certification authorities issue server certificates based on IP addresses, but preliminary evidence indicates that such certificates are a very small percentage (less than 1%) of issued certificates". In order to allow for PKIX-based authentication between a DOTS client and server, this document specifies the DHCP option as a name. One or multiple IP addresses may be returned as a result of name resolution.

Defining the option to include a list of IP addresses would avoid a dependency on an underlying name resolution, but that design requires to also supply a name for PKIX-based authentication purposes.

Because aliasing is to be avoided (Section 7 of [RFC7227]), this document specifies one single option that conveys a DOTS server's name.

This specification assumes that the same name is used to contact the DOTS server for both signal and data channels needs. The selection of the transport protocols to be used and the companion service port numbers are assumed to be by default determined by the DOTS client as specified in [I-D.ietf-dots-signal-channel] and [I-D.ietf-dots-data-channel]. The provisioned DOTS name is passed to

the DOTS client that in its turn pass it to an underlying resolution library (e.g., DNS).

DISCUSSION NOTE: Consider whether the DOTS client proceeds with S-NAPTR lookups.

6.2. DHCPv6 DOTS Option

6.2.1. Format

The DHCPv6 DOTS option is used to configure a name of the DOTS server. The format of this option is shown in Figure 2.

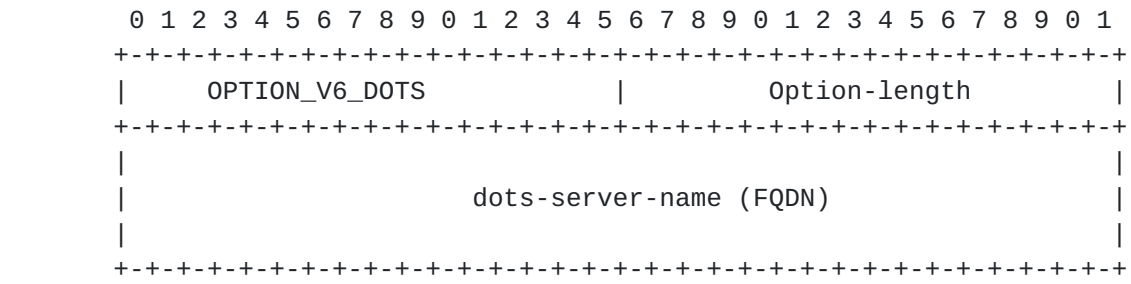


Figure 2: DHCPv6 DOTS option

The fields of the option shown in Figure 2 are as follows:

- Option-code: OPTION_V6_DOTS (TBA, see Section 11.1)
- Option-length: Length of the dots-server-name field in octets.
- dots-server-name: A fully qualified domain name of the DOTS server. This field is formatted as specified in Section 8 of [RFC3315].

An example of the dots-server-name encoding is shown in Figure 3. This example conveys the FQDN "dots.example.com.".

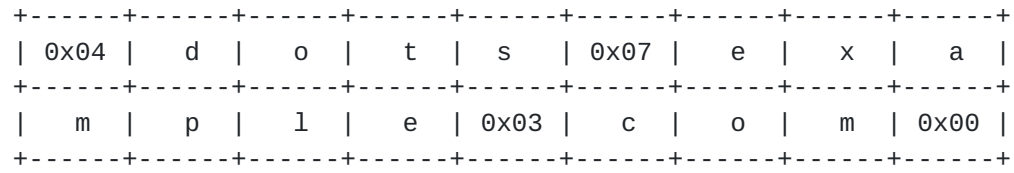


Figure 3: An example of the dots-server-name encoding

6.2.2. DHCPv6 Client Behavior

DHCP clients MAY request option OPTION_V6_DOTS, as defined in [RFC3315], Sections 17.1.1, 18.1.1, 18.1.3, 18.1.4, 18.1.5, and 22.7. As a convenience to the reader, it is mentioned here that the DHCP client includes the requested option codes in the Option Request Option.

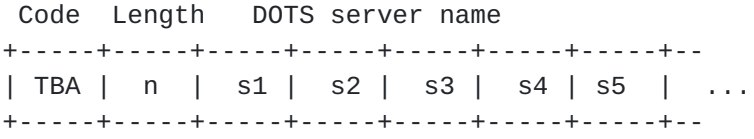
If the DHCP client receives more than one OPTION_V6_DOTS option, it MUST use only the first instance of that option.

If the OPTION_V6_DOTS option contains more than one name, as distinguished by the presence of multiple root labels, the DHCP client MUST use only the first name. Once the name is validated (Section 8 of [RFC3315]), the name is passed to a name resolution library.

6.3. DHCPv4 DOTS Option

6.3.1. Format

The DHCPv4 DOTS option is used to configure a name of the DOTS server. The format of this option is illustrated in Figure 4.



The values s1, s2, s3, etc. represent the domain name labels in the domain name encoding.

Figure 4: DHCPv4 DOTS option

The fields of the option shown in Figure 4 are as follows:

- Code: OPTION_V4_DOTS (TBA, see Section 11.2);
- Length: Includes the length of the "DOTS server name" field in octets; the maximum length is 255 octets.
- DOTS server name: The domain name of the DOTS server. This field is formatted as specified in Section 8 of [RFC3315].

6.3.2. DHCPv4 Client Behavior

To discover a DOTS server, the DHCPv4 client MUST include OPTION_V4_DOTS in a Parameter Request List Option [RFC2132].

If the DHCP client receives more than one OPTION_V4_DOTS option, it MUST use only the first instance of that option.

If the OPTION_V4_DOTS option contains more than one name, as distinguished by the presence of multiple root labels, the DHCP client MUST use only the first FQDN. Once the name is validated (Section 8 of [RFC3315]), the name is passed to a name resolution library.

7. Discovery using Service Resolution

This mechanism is performed in two steps:

1. A DNS domain name is retrieved for each combination of interface and address family.

2. Retrieved DNS domain names are then used for S-NAPTR lookups. Further DNS lookups may be necessary to determine DOTS server IP address(es).

7.1. Retrieving Domain Name

A DOTS client has to determine the domain in which it is located. The following section describes the means to obtain the domain name from DHCP. Other means of retrieving domain names may be used, which are outside the scope of this document, e.g., local configuration.

Implementations MAY allow the user to specify a default name that is used, if no specific name has been configured.

7.1.1. DHCP

DHCP can be used to determine the domain name related to an interface's point of network attachment. Network operators may provide the domain name to be used for service discovery within an access network using DHCP. Sections 3.2 and 3.3 of [RFC5986] define DHCP IPv4 and IPv6 access network domain name options, OPTION_V4_ACCESS_DOMAIN and OPTION_V6_ACCESS_DOMAIN respectively, to identify a domain name that is suitable for service discovery within the access network.

For IPv4, the discovery procedure MUST request the access network domain name option in a Parameter Request List option, as described in [RFC2131]. [RFC2132] defines the DHCP IPv4 domain name option; while this option is less suitable, a client MAY request for it if the access network domain name defined in [RFC5986] is not available.

For IPv6, the discovery procedure MUST request for the access network domain name option in an Options Request Option (ORO) within an Information-request message, as described in [RFC3315].

If neither option can be retrieved the procedure fails for this interface. If a result can be retrieved it will be used as an input for S-NAPTR resolution.

7.2. Resolution

Once the DOTS client has retrieved domain names, an S-NAPTR lookup with 'DOTS' application service and the desired protocol tag is made to obtain information necessary to connect to the authoritative DOTS server within the given domain. S-NAPTR lookup lets the DOTS server administrators provision the preferred DOTS transport protocol between the client and the server and allows the DOTS client to discover this preference.

This specification defines "DOTS" as an application service tag (Section 11.3.1) and "signal.udp" (Section 11.3.2), "signal.tcp" (Section 11.3.3), and "data.tcp" (Section 11.3.4) as application protocol tags.

(Proposal-1)
In the example below, for domain 'example.net', the resolution algorithm will result in IP address(es), port, tag and protocol tuples as follows:

```
example.net.
IN NAPTR 100 10 "" DOTS:signal.udp "" signal.example.net.
IN NAPTR 200 10 "" DOTS:signal.tcp "" signal.example.net.
IN NAPTR 300 10 "" DOTS:data.tcp "" data.example.net.

signal.example.net.
IN NAPTR 100 10 S DOTS:signal.udp "" _dots._signal._udp.example.net.
IN NAPTR 200 10 S DOTS:signal.tcp "" _dots._signal._tcp.example.net.

data.example.net.
IN NAPTR 100 10 S DOTS:data.tcp "" _dots._data._tcp.example.net.

_dots._signal._udp.example.net.
IN SRV   0 0 5000 a.example.net.

_dots._signal._tcp.example.net.
IN SRV   0 0 5001 a.example.net.

_dots._data._tcp.example.net.
IN SRV   0 0 5002 a.example.net.

a.example.net.
IN AAAA  2001:db8::1
```

Order	Protocol	IP address	Port	Tag
1	UDP	2001:db8::1	5000	Signal
2	TCP	2001:db8::1	5001	Signal
3	TCP	2001:db8::1	5002	Data

(Proposal-2)
In the example below, for domain 'example.net', the resolution algorithm will result in IP address(es), port, tag and protocol tuples as follows:

```
example.net.
IN NAPTR 100 10 "" DOTS-SIGNAL:dots.udp "" signal.example.net.
IN NAPTR 200 10 "" DOTS-SIGNAL:dots.tcp "" signal.example.net.
IN NAPTR 300 10 "" DOTS-DATA:dots.tcp "" data.example.net.

signal.example.net.
IN NAPTR 100 10 S DOTS:signal.udp "" _dots._signal._udp.example.net.
IN NAPTR 200 10 S DOTS:signal.tcp "" _dots._signal._tcp.example.net.

data.example.net.
IN NAPTR 100 10 S DOTS:data.tcp "" _dots._data._tcp.example.net.

_dots._signal._udp.example.net.
IN SRV   0 0 5000 a.example.net.

_dots._signal._tcp.example.net.
IN SRV   0 0 5001 a.example.net.

_dots._data._tcp.example.net.
IN SRV   0 0 5003 a.example.net.

a.example.net.
IN AAAA  2001:db8::1
```

Order	Protocol	IP address	Port	Tag
1	UDP	2001:db8::1	5000	Signal
2	TCP	2001:db8::1	5001	Signal
3	TCP	2001:db8::1	5003	Data

If no DOTS-specific S-NAPTR records can be retrieved, the discovery procedure fails for this domain name (and the corresponding interface and IP protocol version). If more domain names are known, the discovery procedure MAY perform the corresponding S-NAPTR lookups immediately. However, before retrying a lookup that has failed, a DOTS client MUST wait a time period that is appropriate for the encountered error (e.g., NXDOMAIN, timeout, etc.).

8. DNS-SD/mDNS

To be completed (if needed).

9. Anycast

IP anycast can also be used for DOTS service discovery. A packet sent to an anycast address is delivered to the 'topologically nearest' network interface with the anycast address.

When a DOTS client requires DOTS services, it attempts to establish a signaling session with the assigned anycast address(es) defined in Sections 11.4 and 11.5. A DOTS server, that receives a DOTS request with an anycast address, SHOULD redirect the DOTS client to the appropriate DOTS unicast server(s) using the mechanism described in Section 5.5 of [I-D.ietf-dots-signal-channel], unless it is configured otherwise. Indeed, a DOTS server SHOULD be configurable to maintain all DOTS communications using anycast. DOTS redirect is not made mandatory because the use of anycast is not problematic for some deployment scenarios such as an enterprise network deploying one single DOTS gateway connected to one single network provider.

[I-D.boucadair-dots-multihoming] identifies a set of deployment schemes in which the use of anycast is not recommended.

10. Security Considerations

DOTS-related security considerations are discussed in Section 4 of [I-D.ietf-dots-architecture].

10.1. DHCP

The security considerations in [RFC2131] and [RFC3315] are to be considered.

10.2. Service Resolution

The primary attack against the methods described in Section 7 is one that would lead to impersonation of a DOTS server. An attacker could attempt to compromise the S-NAPTR resolution. The use of mutual authentication makes it difficult to redirect a DOTS client to an illegitimate DOTS server.

10.3. Anycast

Anycast-related security considerations are discussed in [RFC4786] and [RFC7094].

11. IANA Considerations

11.1. DHCPv6 Option

IANA is requested to assign the following new DHCPv6 Option Code in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters:

Option Name	Value
OPTION_V6_DOTS	TBA

11.2. DHCPv4 Option

IANA is requested to assign the following new DHCPv4 Option Code in the registry maintained in http://www.iana.org/assignments/bootp-dhcp-parameters/:

Option Name	Value	Data length	Meaning
OPTION_V4_DOTS	TBA	Variable; the maximum length is 255 octets.	Includes the name of the DOTS server.

11.3. Application Service & Application Protocol Tags

This document requests IANA to make the following allocations from the registry available at: https://www.iana.org/assignments/s-naptr-parameters/s-naptr-parameters.xhtml.

11.3.1. DOTS Application Service Tag Registration

- Application Protocol Tag: DOTS
- Intended Usage: See Section 7.2
- Security Considerations: See Section 10
- Contact Information: <one of the authors>

11.3.2. signal.udp Application Protocol Tag Registration

- Application Protocol Tag: signal.udp
- Intended Usage: See Section 7.2
- Security Considerations: See Section 10
- Contact Information: <one of the authors>

11.3.3. signal.tcp Application Protocol Tag Registration

- Application Protocol Tag: signal.tcp
- Intended Usage: See Section 7.2
- Security Considerations: See Section 10
- Contact Information: <one of the authors>

11.3.4. data.tcp Application Protocol Tag Registration

- Application Protocol Tag: data.tcp
- Intended Usage: See Section 7.2
- Security Considerations: See Section 10
- Contact Information: <one of the authors>

11.4. IPv4 Anycast

IANA has assigned a single IPv4 address from the 192.0.0.0/24 prefix and registered it in the "IANA IPv4 Special-Purpose Address Registry" [RFC6890].

Attribute	Value
Address Block	TBA
Name	Distributed-Denial-of-Service Open Threat Signaling (DOTS) Anycast
RFC	<this document>
Allocation Date	<date of approval of this document>
Termination Date	N/A
Source	True
Destination	True
Forwardable	True
Global	True
Reserved-by-Protocol	False

11.5. IPv6 Anycast

IANA has assigned a single IPv6 address from the 2001:0000::/23 prefix and registered it in the "IANA IPv6 Special-Purpose Address Registry" [RFC6890].

Attribute	Value
Address Block	TBA
Name	Distributed-Denial-of-Service Open Threat Signaling (DOTS) Anycast
RFC	<this document>
Allocation Date	<date of approval of this document>
Termination Date	N/A
Source	True
Destination	True
Forwardable	True
Global	True
Reserved-by-Protocol	False

12. Acknowledgements

To be completed.

13. References

13.1. Normative References

[I-D.ietf-dots-architecture]
Mortensen, A., Andreasen, F., Reddy, T., christopher_gray3@cable.comcast.com, c., Compton, R., and N. Teague, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Architecture", draft-ietf-dots-architecture-03 (work in progress), June 2017.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <http://www.rfc-editor.org/info/rfc2131>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <http://www.rfc-editor.org/info/rfc2132>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, DOI 10.17487/RFC3958, January 2005, <http://www.rfc-editor.org/info/rfc3958>.

[RFC5986] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, DOI 10.17487/RFC5986, September 2010, <http://www.rfc-editor.org/info/rfc5986>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <http://www.rfc-editor.org/info/rfc6890>.

13.2. Informative References

[I-D.boucadair-dots-multihoming] Boucadair, M. and T. Reddy, "Multi-homing Considerations for Distributed-Denial-of-Service Open Threat Signaling (DOTS)", draft-boucadair-dots-multihoming-00 (work in progress), June 2017.

[I-D.ietf-dots-data-channel] Reddy, T., Boucadair, M., Nishizuka, K., Xia, L., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel", draft-ietf-dots-data-channel-02 (work in progress), June 2017.

[I-D.ietf-dots-signal-channel] Reddy, T., Boucadair, M., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel", draft-ietf-dots-signal-channel-02 (work in progress), June 2017.

[I-D.ietf-dots-use-cases] Dobbins, R., Fouant, S., Migault, D., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling (DDoS) Open Threat Signaling", draft-ietf-dots-use-cases-05 (work in progress), May 2017.

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

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <http://www.rfc-editor.org/info/rfc4786>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <http://www.rfc-editor.org/info/rfc6125>.

[RFC7094] McPherson, D., Oran, D., Thaler, D., and E. Osterweil, "Architectural Considerations of IP Anycast", RFC 7094, DOI 10.17487/RFC7094, January 2014, <http://www.rfc-editor.org/info/rfc7094>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <http://www.rfc-editor.org/info/rfc7227>.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

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

Email: TirumaleswarReddy_Konda@McAfee.com

Prashanth Patil
Cisco Systems, Inc.

Email: praspati@cisco.com