DOTS Working Group
Internet-Draft
Intended status: Informational
Expires: January 8, 2016

A. Mortensen
Arbor Networks, Inc.
July 07, 2015

DDoS Open Threat Signaling Requirements
draft-mortensen-threat-signaling-requirements-00

Abstract

This document discusses the requirements for a protocol sufficient for the goals of the DDoS Open Threat Signaling (DOTS) Working Group.

Table of Contents

1. Introduction

1.1. Overview

As DDoS attack scale and frequency continue to grow, a number of cloud mitigation providers have emerged to offer on-demand traffic scrubbing servicest. Each service offers its own ad hoc interfaces for subscribers to request threat handling, leaving subscribers tied to proprietary implementations that are not portable from service to service. These ad hoc implementations also severely limit the subset of network elements capable of participating in any coordinated attack response.

The current lack of a common method to make inter-domain threat handling requests and share realtime attack telemetry hampers response coordination. The DOTS Working Group has assigned itself the task of standardizing a protocol or protocols to address that lack.

The requirements for these protocols are unusually stringent. The data link between signaling elements may be saturated with attack traffic--likely inbound, but outbound congestion must also be considered--and the signaling elements cannot rely an the availability of an out-of-band channel to report the attack and request threat handling. High packet loss rates are to be expected, rendering every round trip uncertain.

As such, the protocol which DOTS develops or adapts must have certain characteristics tending to increase the probability of signal delivery between endpoints. At the same time, the protocol must be rich enough to support not only simple calls for aid and limited attack telemetry, but also extensibility such that DOTS is adaptable to future needs.

1.2. Conventions

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 [RFC2119].

2. Terminology

The following terms are meant to help define relationships between elements as well as the data they exchange:

2.1. Attack Telemetry

Attack Telemetry is a catch-all term for collected network traffic characteristics defining the nature of a DDoS attack, and which contributes to the detection, classification, traceback, and mitigation of the attack.

In addition to the properties defining IP Traffic Flow as described by [RFC3917], the Attack Telemetry may include information like:

- o traffic rates from attacker sources in packets and bytes per second,
- o detected attack class (e.g., reflection/amplification, resource exhaustion, etc.),
- o attack duration

as well as any other information deemed valuable for attack response by the Working Group.

2.2. Configuration Channel

The Configuration Channel is a RESTful [REST] interface to establish a common understanding of signal and threat handling between the Signaler and Signal Handler. The RESTful interface enables local operator control over DOTS elements.

2.3. Signal Channel

The Signal Channel refers to the bidirectional communication layer established between the Signaler and the Signal Handler, over which Signals and Signal Responses are transmitted.

2.4. Signal

A DOTS Signal is a message sent from a Signaler to a Signal Handler. The Signal carries information necessary to identify the Signaler and communicate Signaler intent, attack insight to the Signal Handler, and indicators useful for measuring Signal Channel Health.

A Signal permits a Signaler to r The Signal is also the vehicle through which a Signaler requests threat handling.

2.5. Signal Response

A DOTS Signal Response is a message sent from Signal Handler to a Signaler. A Signal Response is variation of a Signal, in that it includes data identifying the originating Signal Handler and indicators of Signal Channel Health. The Signal Response will also include information describing the status of any ongoing threat handling undertaken at a Supplicant’s request.

Note that Signal Responses are sent without solicitation by a Signaler. That is, a Signal Handler sends Signal Responses to an established Signaler regardless of whether the Signal Handler has received a Signal message. (See Signal Channel Health below.)

2.6. Signaler

The DOTS endpoint transmitting a Signal to a Signal Handler in order to communicate Attack Telemetry and request or withdraw a request for threat handling. When a Signaler requests threat handling from the Signal Handler, the Signaler is called a Supplicant.

A Signaler MAY establish Signal Channels with multiple Signal Handlers.

2.7. Supplicant

A DOTS Supplicant is a Signaler requesting threat handling from the Signal Handler. The Supplicant is often downstream of the attack from the Signal Handler, so the Supplicant will often be requesting attack response closer to the sources of attack.

2.8. Signal Handler

The DOTS endpoint responsible for processing and responding to Signals received from a Signaler. A Signal Handler may or may not be in the same domain as the Signaler. When a Supplicant requests threat handling, the Signal Handler is responsible for communicating that request to the entities tasked with the attack response. The attack response itself is out of scope for DOTS, but the Signal Handler should transmit Signal Responses with threat handling feedback to the Supplicant.

Note that Signal Handler and Threat Handler are often but not always synonymous.

2.9. Signal Relay

A DOTS node acting as a Signal Handler and a Signaler. In the role of a Signal Handler, a Signal Relay receives Signals from a downstream Signaler, and then acts as a Signaler when relaying the Signal to an upstream Signal Handler. A Signal Relay also relays any responses from upstream to the originating Signaler.

2.10. Threat Handler

The Threat Handler is the entity or collection of entities tasked with handling an attack at the request of a Supplicant. The Threat Handler and Signal Handler may be one and the same, but are not required to be.

3. Protocol

This section examines requirements for successful threat signaling.

The Working Group has thus far focused attention on adapting IPFIX as a possible vehicle for the DOTS protocol. The expectation as described in [I-D.teague-open-threat-signaling] is that IPFIX's templating system will provide DOTS the necessary flexibility and extensibility, while the wide availability of IPFIX will lower the bar for adoption among vendors. The IANA registry of IPFIX Informational Entities [IANA-IPFIX-IE] similarly increases the appeal of IPFIX by eliminating the need to define a variety of field types.

However, the ultimate selection of IPFIX as the foundation of the DOTS protocol is by no means certain at this stage. It is our hope that by reaching a common understanding of protocol requirements the Working Group will be able to make rapid progress defining the protocol itself.

3.1. Operation

One of the unusual aspects of DOTS is that it depends not so much on protocol reliability but on protocol resiliency. Signal lossiness, to a greater or lesser degree, is to be expected, and the protocol must continue to operate regardless.

DOTS should be able to absorb the loss of multiple consecutive Signals or Signal Responses and still operate nominally, relying on measures like redundant message transmission to increase the likelihood of successful delivery. By the same token, the protocol demands the DOTS nodes share a common understanding of a failed signal channel.

This section discusses the protocol characteristics required to achieve the necessary resiliency, while also retaining the signal effectiveness sought by the Working Group.

3.1.1. Endpoint Communication

A synchronous message-oriented protocol is ill-suited for the conditions under which DOTS is expected to operate. Such a protocol would require a level of reliable message delivery in either direction that we cannot depend on for DOTS.

In contrast, an asynchronous message-oriented protocol fits DOTS requirements, offering resiliency even when dealing with a high level of signal lossiness. As long as the protocol includes indicators showing the time or sequence of the last message received by the peer, each endpoint can continue signaling, and incorporate the most recent data from its peer when messages arrive.

In practice, the Signaler sends messages to the Signal Handler, regardless of responses from Signal Handler, and the Signal Handler does the same in the opposite direction. Until an endpoint detects fail health continue to arrive at each endpoint, DOTS is operational.

3.1.1.1. Signal Channel Health

Monitoring signal delivery success rates is vital to normal DOTS operations. The protocol SHOULD include a way for each endpoint to detect when their respective peers last received a message. This could be achieved through inclusion of timestamps or sequence numbers in the signal messages.

With this method for detecting signal lossiness in place, any received DOTS message acts as a signal heartbeat, meaning no additional keep-alive messages are needed.

Should too much time elapse since an endpoint last received a message from its peer, the endpoint SHOULD consider the peer unresponsive, and in some way alert the operator to the loss of signal. Similarly, if messages continue to arrive from the peer, but the timestamp or sequence number do not update in spite of repeated message transmissions to the peer, the signal MUST be considered degraded, and an appropriate alert should be delivered to the operator.

The method of alerting is out of scope. The endpoints may agree upon the signal failure time-to-live using the configuration channel.

3.1.2. Message Frequency

TODO

3.1.3. Redundant Signal Channels

A Signaler may wish to establish Signal Channels with multiple Signal Handlers in the same domain to increase the likelihood that a Supplicant request for threat handling will be honored.

3.1.4. Redundant Transmission

The likelihood of packet loss due to congestion caused by, for example, a volumetric attack diminishes the resiliency of the protocol. A low-cost method to increase the probability of successful message delivery is through redundant message transmission at send time.

3.2. Transport

As noted above, the DOTS signal protocol does not require reliable, in-order delivery to be effective. The protocol may indeed become less reliable in the attempt to ensure all signal messages are delivered in the order sent, as pathological network conditions lead to missed delivery acknowledgments from the peer. In the worst case, none of the transport acknowledgements reach the signaler, resulting in spurious dead peer detection and subsequent connection teardown.

As such, it is RECOMMENDED that the DOTS protocol use connectionless transports like the User Datagram Protocol (UDP) [RFC0768]. While UDP imposes some additional work on the protocol, the minimal overhead for transmission aligns with DOTS requirements for protocol resiliency.

3.2.1. Congestion Control Considerations

A DOTS signal channel will not contribute to link congestion, as the protocol's transmission rate will be negligible regardless of network conditions.

3.2.2. Alternative Transport Considerations

Where additional constraints imposed by middlebox limitations, overly aggressive filtering, or network policy disqualify UDP, TCP MAY be used for the Signal Channel. However, TCP remains a poor choice for inter-domain signaling over a saturated link for the reasons described above, and consideration should be given to using a Signal Relay between the Signaler and the remote domain's Signal Handler.

3.2.3. Message Size

DOTS protocol messages MUST be smaller than the path maximum transmission unit (MTU) to avoid fragmentation. In the lossy network conditions under which DOTS is expected to operate, fragmentation unnecessarily increases the likelihood of message delivery failure, as a single lost fragment will cause the entire message to be discarded.

3.2.4. Transport Security

The DOTS Working Group charter describes the need to ensure "appropriate regard for authentication, authorization, integrity, and authenticity" in any developed or adapted protocols.

3.2.4.1. DTLS

On the surface, Datagram Transport Layer Security [RFC6347] would seem to be the obvious choice to meet those requirements. However, the conventional three-way TLS handshake using public-key infrastructure incurs significant overhead. The elevated likelihood of handshake failure due to saturated links or otherwise hostile network conditions may be unacceptable for DOTS.

Some of this overhead may be eliminated using preshared keys (e.g., [RFC5487] and [RFC5489]), but the round-trip overhead of the three-way handshake is less easily overcome. The current drafts for TLS 1.3 [I-D.ietf-tls-tls13] make some headway in this regard, introducing a 1-RTT TLS handshake. This is a vast improvement for DOTS operations, but the timeline for standardization and vendor implementation is uncertain.

Regardless of TLS handshake innovation, DTLS by itself lacks a way to detect dead peers. The DTLS Heartbeat Extension [RFC6520] resolves this, but represents an another messaging layer likely to be affected by network lossiness. In addition, the DTLS Heartbeat extension requires immediate responses to heartbeat requests, with the requester retransmitting up to the limit defined in [RFC6347]. The DTLS Heartbeat Extension indicates a DTLS session SHOULD be terminated if the peer does not respond after the retransmission limit is reached. Given the unpredictability of message delivery in the typical DOTS scenario, this rigidity only adds to concerns about the aptness of DLTS for DOTS transport security.

3.2.4.2. Continued Evaluation

The DOTS Working Group will need to evaluate available options for meeting the goal of providing protocol confidentiality, integrity, and authenticity. Guidance should be sought from the TLS Working Group as appropriate.

Guidance and insight may also be found in the DTLS in Constrained Environments [DICE] Working Group. The DICE WG is currently evaluating and developing techniques for transport security in network conditions that may be similar to those in which DOTS will need to work.

3.3. Message Data

As we note above, the Working Group has thus far focused on the suitability of IPFIX as the DOTS signaling protocol. This section makes no judgment in that regard.

3.3.1. Signal

In addition to the requirements laid out in the Protocol Operation, section the Signal MUST be able to:

- provide such attack telemetry as is available to the signaler,
- permit the signaler to request or withdraw a request for intervention from the signal receiver,
- permit the signaler to request refinement or expansion of the scope of threat handling performed by the signal receiver,
- allow customization to the extent required to adapt to emerging requirements or local needs.

3.3.2. Signal Response

In addition to the requirements laid out in the Protocol Operation section, the Signal Response SHOULD deliver feedback to the signaler from the entity or entities handling a threat on the signaler's behalf.

Feedback would include threat handling status, threat handling scope, blocked packet and byte counters, and so on.

4. Configuration Channel

The Configuration Channel would permit local operator control over threat handling by a Signal Handler.

Configurable features might include:

- Signaler address space protection preferences
- Static Black/White lists to apply during threat handling
- UUID assigned to the Signaler by the Signal Handler, which the Signaler must include in subsequent Signals
- Other information not well-suited to transmission under attack conditions

4.1. Configuration Protocol

An obvious choice for the configuration protocol is a RESTful interface over a secure HTTP [RFC2616] channel. Such interfaces are well-understood and easily adopted. With configuration as a concern, [I-D.ietf-netconf-restconf] may be a good fit for DOTS configuration needs.

5. IANA Considerations

TODO

6. Security Considerations

The DOTS Working Group was formed to standardize methods for realtime inter-domain threat signaling. Any protocols must therefore be capable of transmitting information over public networks, with consequent requirements for message integrity, confidentiality, and authenticity.

Transport security and message authenticity are addressed above. In the event either is compromised, regardless of the method involved, the security risks exposed include:

- attack telemetry forgery
- threat handling request forgery
- Denial of Service (DoS) attacks

In scenarios in which DOTS endpoints are communicating across public networks, the endpoints are themselves subject to attack. Endpoint operators SHOULD take steps to restrict access as much as possible to known valid peers through application of network policy and peer authentication.

TODO

7. Acknowledgments

Roland Dobbins deserves full credit for suggesting the Signal Relay, as well as thanks for his insight and his generosity with his time as we discussed the topics that led to this draft.

Thanks to Larry Huston, Sean O’Hara, and David Watson for discussions and support.

8. References

8.1. Normative References

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC3917] Quittek, J., Zseby, T., Claise, B., and S. Zander, "Requirements for IP Flow Information Export (IPFIX)", RFC 3917, October 2004.

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009.

[RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5489, March 2009.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6520] Seggelmann, R., Tuexen, M., and M. Williams, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension", RFC 6520, February 2012.

[I-D.ietf-netconf-restconf]
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-07 (work in progress), July 2015.

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-07 (work in progress), July 2015.

[I-D.teague-open-threat-signaling]
Teague, N., "Open Threat Signaling using RPC API over HTTPS and IPFIX", draft-teague-open-threat-signaling-01 (work in progress), July 2015.

8.2. Informative References

[DICE] "DTLS in Constrained Environments", July 2015, <https://datatracker.ietf.org/wg/dice/charter/>.

[IANA-IPFIX-IE]
"IP Flow Information Export (IPFIX) Entities", April 2015, <http://www.iana.org/assignments/ipfix>.

[REST] Fielding, R., "Architectural Styles and the Design of Network-based Software Architectures", 2000, <https://www.ics.uci.edu/˜fielding/pubs/dissertation/top.htm>.

Author's Address

Andrew Mortensen
Arbor Networks, Inc.
2727 S. State St
Ann Arbor, MI 48104
United States

Email: amortensen@arbor.net