Transmission of SYSLOG message over DTLS
draft-feng-syslog-transport-dtls-00.txt

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 29, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Abstract

This document describes a Transport for the Syslog Protocol, which uses the Datagram Transport Layer Security (DTLS) protocol. The DTLS protocol provides authentication and privacy services for SYSLOG applications. This document describes how using DTLS to transport SYSLOG messages makes this protection possible in an interoperable way.

This transport is designed to meet the security and operational needs of network administrators, operate in environments where a connectionless (UDP) transport is preferred, and integrates well into existing public keying infrastructures.

Table of Contents

1. Introduction .............................................. 3
2. Terminology .............................................. 3
3. Threats ..................................................... 4
4. Using DTLS to Secure Syslog .............................. 5
   4.1. Security ............................................ 5
   4.2. Security Policies ................................... 5
   4.3. Transport ............................................ 5
5. Message Process .......................................... 5
   5.1. Port .................................................. 6
   5.2. Message Size ........................................ 6
   5.3. Session Demultiplexing ............................... 6
      5.3.1. Outgoing Message Process ....................... 6
      5.3.2. Incoming Message Process ...................... 6
6. Applicable Scenarios .................................... 7
7. Security Considerations .................................. 7
   7.1. Authentication of message origin ................... 7
   7.2. Reliability .......................................... 7
   7.3. Reordering .......................................... 8
   7.4. Congestion Control .................................. 8
8. IANA Consideration ...................................... 8
9. Acknowledgements ....................................... 8
10. References ............................................. 8
   10.1. Normative References ............................... 8
   10.2. Informative References ............................. 9
1. Introduction

The Syslog protocol [I-D.ietf-syslog-protocol] is designed to run over different transports for different environments. [I-D.ietf-syslog-tls] provides a combination of TCP transport reliability with TLS security [RFC5246].

However, TCP performance can be a problem when a network has a high rate of lost packets. In these circumstances, an operator might prefer using UDP to TCP as transport. [I-D.ietf-syslog-UDP] defines how to transport SYSLOG over UDP, which provides unreliable, non-secure transport for SYSLOG.

The datagram transport layer security protocol (DTLS) [RFC4347] is designed to meet the requirements of applications that need secure datagram transport, by combining UDP transport with TLS security [RFC5246].

This document describes how to use SYSLOG with a DTLS transport.

2. Terminology

The following definitions from [I-D.ietf-syslog-protocol] are used in this document:

- A "transport sender" passes SYSLOG messages to a specific transport protocol.
- A "transport receiver" takes SYSLOG messages from a specific transport protocol.
- A "DTLS client" is an application that can initiate a DTLS Client Hello to a server.
- A "DTLS server" is an application that can receive a Client Hello from a client and reply with a Server Hello.

The term "session" used in this document is used to refer to a secure association between transport sender and transport receiver that permits the transmission of one or more SYSLOG messages within the lifetime of the session.

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].
3. Threats

Syslog message may transmit in a manner of hop-by-hop, the threats during the transmission have been addressed in [I-D.ietf-syslog-tls]:

The primary threats for SYSLOG are:

- **Masquerade.** An unauthorized transport sender may send messages to a legitimate transport receiver, or an unauthorized transport receiver tries to deceive a legitimate transport sender into sending SYSLOG messages to it.

- **Modification.** An attacker between the transport sender and the transport receiver may modify an in-transit SYSLOG message and then forward the message to the transport receiver. Such modification may make the transport receiver misunderstand the message or cause it to behave in undesirable ways.

- **Disclosure.** An unauthorized entity may examine the contents of the SYSLOG messages, gaining unauthorized access to the information. Some data in SYSLOG messages is sensitive and may be useful to an attacker, such as the password of an authorized administrator or user.

A secondary threat is:

- **Message stream modification.** An attacker may delete one or more SYSLOG message from a series of messages, replay a message, or alter the delivery sequence. The SYSLOG protocol itself is not based on message order, but an event in a SYSLOG message may relate semantically to events in other messages, so message ordering may be important to understanding a sequence of events.

The following secondary threat is addressed in this document:

- **Denial of Service.** Denial of service is addressed in [I-D.ietf-syslog-protocol], which states that attacker may send greater messages to transport receiver than the transport receiver could handle. When using a secure transport protocol, a kind of denial of service could be addressed during handshake that attacker may use a spoofed IP source request for server’s certificate information to consume server’s resource.

The following threat is deemed to be of lesser importance for SYSLOG, and is not addressed in this document:

- **Traffic Analysis**
4. Using DTLS to Secure Syslog

4.1. Security

DTLS can be used as a secure transport to counter all the primary threats to SYSLOG described above:

- Confidentiality to counter disclosure of the message contents;
- Integrity checking to counter modifications to a message on a hop-by-hop basis;
- Server or mutual authentication to counter masquerade.

The extra security features that DTLS can provide:

- A cookie exchange mechanism during handshake to counter Denial of Service attacks
- A sequence number in the header to counter replay attacks.

4.2. Security Policies

Syslog transport over DTLS has been designed to minimize the security and operational differences for environments where both [I-D.ietf-syslog-tls] and SYSLOG over DTLS are supported. The security policies for SYSLOG over DTLS are the same as those described in [I-D.ietf-syslog-tls].

When a transport sender initiate a hello request to a transport receiver, cookie exchange mechanism (borrow from Internet Key Exchange [RFC2521] ) is RECOMMENDED for transport receiver to use to mitigate Denial of Service by spoofed IP address.

4.3. Transport

With DTLS transport, each message is secure and private within the lifetime of a session. TLS can use the TCP connection identifier to identify a session, and to uniquely associate messages with a session ID. DTLS does not provide an association mechanism to identify which message belongs to which session. An implementer SHOULD support session demultiplexing.

5. Message Process
5.1. Port

A SYSLOG transport sender is always a DTLS client and a transport receiver is always a DTLS server. Any UDP port could be configured by the user to send or receive SYSLOG message. The SYSLOG receiver MUST support listening on the default port which IANA assigned for SYSLOG over DTLS, but MAY be configurable to listen on a different port.

5.2. Message Size

Syslog message size mapping for DTLS is limited by the length of application data part in dtls protocol; each dtls message must fit within one datagram, as stated in [RFC4347]. To avoid IP fragmentation, the total datagram size (including IP/UDP/DTLS overhead) MUST not be larger than the MTU (1500 for Ethernet) or the current MTU when using MTU discovery mechanism, nor smaller than the minimum MTU (576 for Ethernet). From this integrity and encryption overhead also needs to be taken into account, which are integrity and encryption algorithm specific.

5.3. Session Demultiplexing

Sessions demultiplexing includes the necessary process for transport sender sending a message and transport receiver receiving a message. There can be different implementation to achieve association of messages received with a session, the implementer SHOULD maintain the mapping relationship between messages and sessions during the session lifetime.

5.3.1. Outgoing Message Process

For a SYSLOG transport sender, the messages from application will be treated as the application data by DTLS in the record layer. When there is different security policy mapping on different sessions, the transport sender MUST use different sending port for the transport receiver to distinguish which session it belongs.

5.3.2. Incoming Message Process

A SYSLOG transport receiver MUST decide which an incoming message belongs to which session. Each session identified by a session id in DTLS, maintains a series of security parameters, which is used to decrypt the message in secret to the application in upper layer. DTLS does not support multi-session, which means, DTLS does not provide equivalent method to associate an incoming message with a session id. The application implementer SHOULD resolve it. Usually, an Address-Port pair (source address, source port, destination
address and destination port) could be used to decide a unique session. When the destination address and destination port is decided, different source port can be used to identify different session from same source address.

6. Applicable Scenarios

Syslog over DTLS is applicable in such scenarios as below:

1. In managed networks, the environment where UDP transport is applicable and security is required, where the network path has been explicitly provisioned for UDP SYSLOG traffic through traffic engineering mechanisms, such as rate limiting or capacity reservations. Reference from [I-D.ietf-syslog-UDP].

2. In network environment where using congestion control mechanism, SYSLOG application can benefit from a UDP-based approach rather than a TCP-based approach.

2.1 Bulk transmission of logs: SYSLOG over dtls has more lower delay and lower overhead that could meet the great amount of logs delivery situation.

2.2 The logs transmission is kind of intermittent: keeping TCP connections alive for an occasional poll is not necessarily a good approach. Trying to connection each time in transmission could incur the overhead of TCP connection, especially setting up a TCP connection to get one SYSLOG message.

7. Security Considerations

7.1. Authentication of message origin

This secure transport (i.e., DTLS) only secures SYSLOG transport in a hop-by-hop manner, and is not concerned with the contents of SYSLOG messages. In particular, the authenticated identity of the transport sender (e.g., subject name in the certificate) is not necessarily related to the HOSTNAME field of the SYSLOG message. When authentication of SYSLOG message origin is required, [I-D.ietf-syslog-sign] can be used.

7.2. Reliability

DTLS is a UDP-based transport protocol, which has no reliability mechanism. So, the message could be lost.
7.3. Reordering

Each SYSLOG message is delivered by DTLS record protocol, which has assigned a sequence number for each DTLS record. Although the DTLS implementer may adopt Queue mechanism to resolve reordering, it does not assure that all the messages delivered in order.

7.4. Congestion Control

The transport mapping on DTLS does not provide congestion control mechanism, so, SYSLOG transport over DTLS have the same congestion control problems with transport over UDP. [I-D.ietf-syslog-UDP] has state such problems, when generated unlimited amounts of log transport on the internet, could influence the stable operation of the internet. [RFC5405] has guideline for an application SHOULD perform congestion control over UDP transport, referring to [RFC5405] for details.

Datagram Congestion Control Protocol [RFC4340] is designed and is usually be thought as UDP plus congestion control, which builds-in congestion control mechanism for datagram. DTLS can run over DCCP, [RFC5238] (Datagram Transport Layer Security over the Datagram Congestion Control Protocol) states such combination. To respond to congestion and establish a degree of fairness [RFC2914], it is RECOMMENDED that the implementer also support DCCP [RFC4340] for DTLS to provide congestion control.

8. IANA Consideration

IANA is requested to assign a registered UDP port number for SYSLOG over DTLS.

9. Acknowledgements

Much of this document draws heavily from [I-D.ietf-syslog-tls]. The draft also borrow from Wes Hardaker’s [I-D.hardaker-isms-dtls-tm], when using dtls as transport, SYSLOG and SNMP face same situation to resolve. Particular thanks are due to David Harring for thorough review, who gives great much direction and suggestion, the author is very grateful.

10. References

10.1. Normative References

[I-D.ietf-syslog-UDP] Okmianski, A., "Transmission of SYSLOG messages over UDP", draft-ietf-syslog-transport-UDP-12 (work...
in progress) (work in progress), September 5 2007.

draft-ietf-syslog-protocol-23 (work in progress) (work in progress),
March 2005.

[I-D.ietf-syslog-tls] Miao, F., Ma, Y., and J. Salowey, "TLS
Transport Mapping for Syslog",
draft-ietf-syslog-transport-tls-14 (work in progress) (work in progress),
September 30 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs
to Indicate Requirement Levels",

[RFC2914] Floyd, S., "Congestion Control
Principles", BCP 41, RFC 2914,
September 2000.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram
Transport Layer Security", RFC 4347,
April 2006.

10.2. Informative References

[I-D.hardaker-isms-dtls-tm] Hardaker, W., "Datagram Transport Layer
Security Transport Model for SNMP",
draft-hardaker-isms-syslog-tm-02 (work in progress), December 2008.

[I-D.ietf-syslog-sign] Kelsey, J., Callas, J., and A. Clemm,
"Signed SYSLOG Messages",

[RFC4340] Kohler, E., Handley, M., and S. Floyd,
"Datagram Congestion Control Protocol
(DCCP)", RFC 4340, March 2006.

[RFC5238] Phelan, T., "Datagram Transport Layer
Security (DTLS) over the Datagram
Congestion Control Protocol (DCCP)",

Author’s Address

Hongyan. Feng
Huaweisymantec, Inc.

EMail: fenghongyan@huawei.com