Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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 May 25, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes the use of Transport Layer Security (TLS) to provide a secure connection for the transport of Syslog messages. This document describes the security threats to Syslog and how TLS can be used to counter such threats.
# Table of Contents

1. Introduction ................................................. 3
   1.1. Terminology ............................................. 3
2. Security Requirements for Syslog ............................... 3
3. TLS to Secure Syslog .......................................... 4
4. Protocol Elements ............................................ 5
   4.1. Port Assignment ......................................... 5
   4.2. Initiation ................................................ 5
   4.3. Sending data ............................................. 6
      4.3.1. Frame Length ........................................ 6
      4.3.2. Version .............................................. 7
   4.4. Closure .................................................. 7
5. Security Consideration .......................................... 7
   5.1. Authentication ........................................... 7
5.2. Generic Certificate ......................................... 8
6. IANA Consideration ............................................ 8
   6.1. Port Number ............................................... 8
   6.2. VERSION .................................................. 8
7. Acknowledgments ................................................ 9
8. References .................................................... 9
   8.1. Normative References ..................................... 9
   8.2. Informative References ................................... 9
Authors’ Addresses ............................................... 9
Intellectual Property and Copyright Statements .................. 11
1. Introduction

This document describes the use of Transport Layer Security (TLS [6]) to provide a secure connection for the transport of Syslog messages. This document describes the security threats to Syslog and how TLS can be used to counter such threats.

1.1. Terminology

The following definitions are used in this document:

- A sender is an application that can generate and send a Syslog [2] message to another application.
- A receiver is an application that can receive a Syslog message.
- A relay is an application that can receive Syslog messages and forward them to another receiver.
- A collector is an application that can receive messages but does not relay them to any other receiver.
- A TLS client is an application that can initiate a TLS connection by sending a Client Hello to a peer.
- A TLS server is an application that can receive a Client Hello from a peer and reply with a Server Hello.

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 [1].

2. Security Requirements for Syslog

Syslog messages may pass several hops to arrive at the intended receiver. Some intermediary networks may not be trusted by the sender/relay, receiver, or all because the network is in a different security domain or at a different security level from the receiver, relay, or sender. Another security concern is that the sender/relay, or receiver itself is in an insecure network.

There are several threats to be addressed for Syslog security. The primary threats are:

- Masquerade. An unauthorized sender/relay may send messages to a legitimate receiver, or an unauthorized receiver tries to deceive a legitimate sender/relay into sending Syslog messages to it.
Modification. An attacker between the sender/relay and receiver may modify an in-transit Syslog message from the sender/relay and then forward the message to receiver. Such modification may make the receiver misunderstand the message or cause the receiver to behave in undesirable ways.

Disclosure. An unauthorized entity may examine the content 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.

The secondary threat is:

Message stream modification. An attacker may delete a Syslog message from a series of messages, replay a message or alter the delivery sequence. 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 threats are deemed to be of lesser importance for Syslog, and are not addressed in this document:

- Denial of Service
- Traffic Analysis

3. TLS to Secure Syslog

TLS can be used as a secure transport to counter all the primary and secondary threats to Syslog described in section 2:

- Confidentiality to counter disclosure of the message contents
- Integrity check to counter modifications to a message
- Peer authentication to counter masquerade
- Sequence number along with integrity check to counter message stream modification

The security service is also applicable to BSD Syslog defined in RFC3164 [7]. But, it is not ensured that the protocol specification defined in this document is applicable to BSD Syslog.
4. Protocol Elements

4.1. Port Assignment

A Syslog sender/relay is always a TLS client and a Syslog receiver is always a TLS server.

The TCP port NNN has been allocated as the default port for Syslog over TLS, as defined in this document.

Note to RFC Editor: please replace NNN with the IANA-assigned value, and remove this note.

4.2. Initiation

The sender/relay should initiate a connection to the receiver and then send the TLS Client Hello to begin the TLS handshake. When the TLS handshake has finished the sender/relay may then send the first Syslog message.

TLS uses certificate [4] to authenticate the peers. When a sender/relay authenticates a receiver it MUST validate the certificate. It SHOULD check the common name (CN) of the certificate against the host name of the receiver if it has knowledge of a common name/host name mapping. If the common name does not match the host name, the sender/relay SHOULD send an "access_denied" error alert using the TLS alert protocol to terminate the handshake, and then it SHOULD close the connection.

When a receiver authenticates a sender/relay, the receiver MUST validate the certificate. A sender’s (or relay’s) certificate may be:

- An unique certificate, which is issued to a host and whose Common Name may be host name, IP address, MAC, or device ID.
- A generic certificate, which is issued to a class of application or device. For example, all cable modems from a vendor may be issued the same generic certificate.

A sender/relay certificate may be issued by an operator when a device/application is being provisioned or by a vendor when the device/application is manufactured. This document does not define how the sender/relay certificate is issued.

Syslog applications SHOULD be implemented in a manner that permits administrators to select the cryptographic level they desire. It SHOULD be an administrator decision, as a matter of local policy,
what security level (e.g. cryptographic algorithms and length of keys) is required.

TLS permits the resumption of an earlier TLS session or the use of another active session when a new session is requested, in order to save the expense of another full TLS handshake. The security parameters of the resumed session are reused for the requested session. The security parameters SHOULD be checked against security requirement of requested session to make sure the resumed session provides proper security.

4.3. Sending data

All Syslog messages MUST be sent as TLS "application data". It is possible that there are multiple Syslog messages in one TLS record, or a Syslog message is transferred in multiple TLS records. The application data is defined with the following ABNF [5] expression:

APPLICATION-DATA = VERSION SP 1*SYSLOG-FRAME
VERSION = NONZERO-DIGIT *1DIGIT
SYSLOG-FRAME = FRAME-LEN SP SYSLOG-MSG
FRAME-LEN = NONZERO-DIGIT *DIGIT
SP = " "
DIGIT = "0" / NONZERO-DIGIT
NONZERO-DIGIT = %x31-39
SYSLOG-MSG is defined in Syslog [2] protocol.

4.3.1. Frame Length

The frame length is the octet count of a SYSLOG frame including the FRAME-HEADER and SP parts. A receiver MUST use the frame length field to delimit a Syslog message. There is no upper limit for a frame length per se. However, in order to establish a baseline for interoperability, the specification requires that a receiver MUST be able to process frame with size up to and including 2048 octets. It SHOULD be able to receive frame with size up to and including 8192 octets.
4.3.2. Version

The version is to identify the version of the TLS transport mapping for Syslog, and the version is 1.

If a receiver does not support the version in the messages it received, it MAY just save the APPLICATION-DATA in local storage or send a close_notify to signal the closure of the connection. If a sender/relay finds connections are closed just after successful TLS handshake for three times with same transport mapping version, it SHOULD not connect the receiver again with the same transport mapping version.

4.4. Closure

A Syslog sender/relay MUST close the associated TLS connection if the connection is not expected to deliver Syslog message later. It MUST send a TLS close_notify alert before closing the connection. A sender/relay MAY choose not to wait for the receiver’s close_notify alert and simply close the connection, thus generating an incomplete close on the receiver side. Once the receiver gets close_notify from the sender/relay, it MUST reply with a close_notify unless it becomes aware that the connection has already been closed by the sender/relay (e.g., the closure was indicated by TCP).

When no data is received from a connection for a long time (where the application decides what "long" means), a receiver MAY close a connection. The receiver MUST attempt to initiate an exchange of close_notify alerts with the sender/relay before closing the connection. Receivers those are unprepared to receive any more data MAY close the connection after sending the close_notify alert, thus generating an incomplete close on the sender/relay side. When the sender/relay has received the close_notify alert from the receiver and still has pending data to send, it SHOULD send the pending data before sending the close_notify alert.

5. Security Consideration

5.1. Authentication

TLS supports three authentication modes: authentication of both parties, server authentication with an unauthenticated client, and total anonymity.

TLS authentication and the establishment of secrets is based on certificates and asymmetric cryptography. This makes TLS transport much more expensive than non-TLS plain transport. An attacker may
initialize many TLS connections to a receiver as a denial of service attack. Since a receiver may act upon received data, for Syslog over TLS, the receiver SHOULD authenticate the sender/relay to ensure that information received is authentic.

When confidentiality is a concern, a sender/relay MUST authenticate the receiver to make sure it is talking to the right peer.

5.2. Generic Certificate

When a certificate is issued to a class of device or application, the certificate may be shared by multiple hosts. Multiple hosts know the private key of the certificate. When the certificate in one host is compromised, then the certificate for all hosts that share the certificate is compromised. An attacker may impersonate a legitimate sender to send Syslog message to a receiver.

6. IANA Consideration

6.1. Port Number

IANA is requested to assign a TCP port number in the range 1..1023 in the http://www.iana.org/assignments/port-numbers registry which will be the default port for Syslog over TLS, as defined in this document.

6.2. VERSION

IANA must maintain a registry of VERSION values as described in Section 4.3.2. Version numbers MUST be incremented for any new Syslog TLS transport mapping specification that changes any part of the frame or other parts. Changes include addition or removal of fields or a change of syntax or semantics of existing fields.

VERSION numbers must be registered via the Standards Action method as described in RFC2434 [3]. IANA must register the VERSIONs shown in table 1.

+---------+---------------------------------+
| VERSION | FORMAT                          |
+---------+---------------------------------+
| 1       | According to this specification |
+---------+---------------------------------+

Table 1: Version Number
7. Acknowledgments

Authors appreciate Eric Rescorla, Anton Okmianski, Rainer Gerhards, Balazs Scheidler and Chris Lonvick for their effort on issues resolving discussion. Authors would also like to appreciate Balazs Scheidler, Tom Petch and other persons for their input on security threats of Syslog. The author would like to acknowledge David Harrington for his detailed reviews of the content and grammar of the document.

8. References

8.1. Normative References


8.2. Informative References

Authors’ Addresses

Miao Fuyou
Huawei Technologies
No. 3, Xinxi Rd
Shangdi Information Industry Base
Haidian District, Beijing 100085
P. R. China

Phone: +86 10 8288 2008
Email: miaofy@huawei.com
URI: www.huawei.com

Ma Yuzhi
Huawei Technologies
No. 3, Xinxi Rd
Shangdi Information Industry Base
Haidian District, Beijing 100085
P. R. China

Phone: +86 10 8288 2008
Email: myz@huawei.com
URI: www.huawei.com