TRANS
Internet-Draft
Intended status: Experimental
Expires: April 30, 2015

L. Nordberg
NORDUnet

October 27, 2014

Transparency Gossip HTTPS transport
draft-linus-trans-gossip-transport-https-00

Abstract

This document specifies a [draft-linus-trans-gossip] transport protocol for sending Transparency Gossip messages over https.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 30, 2015.

Copyright Notice

Table of Contents

1. Introduction

Using web servers as "gossip pools" is expected to be helpful for transparency gossiping, especially for [RFC6962].

Web browsers can act as an HTTPS transport, sending and receiving gossip messages to web servers it connects to for other reasons than gossiping.

HTTPS transports that don't have connections to web servers for other reasons than gossiping may connect to web servers known to support gossiping. They can be known by configuration or by other mechanisms. This document does not specify such mechanisms.

2. Sending and receiving

Gossip messages may contain sensitive information and MUST NOT be sent over connections which are not encrypted as described in [RFC2817] or [RFC2818] using TLS version 1.0 or higher. When applicable the server SHOULD be authenticated using X.509 certificates as described in [RFC2459] or by other means.

HTTPS gossip messages are sent in [RFC2616] message headers with the field-name "TransGossip".

An HTTPS transport

- SHOULD send gossip messages to HTTP servers that have indicated that they accept gossip by sending an HTTP response-header "TransGossipEnabled" with the value "Yes"

- MAY send gossip messages to HTTP servers that haven't indicated willingness to accept gossip

- MUST NOT send gossip messages to HTTP servers that have indicated that they don't accept gossip by sending an HTTP response-header "TransGossipEnabled" with the value "No"

3. Message format and processing

Messages are strings of US-ASCII data on the following form:

<protocol-version>:<log-id>:<gossip-data>

'protocol-version' is the version number of the protocol in decimal. This version is 0.

'log-id' and 'gossip-data' are as defined in the GOSSIP-MSG of [draft-linus-trans-gossip]. Note that 'gossip-data' is base64-encoded.

Messages MUST be processed according to [draft-linus-trans-gossip].

[FIXME are there any http specific processing rules to be added?]

4. Security considerations

TBD

5. IANA considerations

TBD

6. Contributors

The author would like to thank Ben Laurie for their valuable contributions.

7. References

7.1. Normative References

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

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

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC2459] Housley, R., Ford, W., Polk, T., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[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.

[RFC2817] Khare, R. and S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC 2817, May 2000.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[draft-linus-trans-gossip] "Transparency Gossip", n.d..

7.2. Informative References

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, June 2013.

Author's Address

Linus Nordberg
NORDUnet

Email: linus@nordu.net