Network Working Group M. Miller
Internet-Draft Cisco Systems, Inc.
Intended status: Informational January 23, 2014
Expires: July 27, 2014

Applying Unauthenticated Transport Layer Security (TLS) to Hypertext Transport Protocol (HTTP) Connections
draft-miller-http-unauth-tls-00

Abstract

With the pervasiveness of passive monitoring and ubiquity of unencrypted Hypertext Transport Protocol (HTTP), it is desirable to mitigate passive monitoring without causing an undue burden on HTTP user agents and servers. This document describes the rationale and process for using Transport Layer Security (TLS) in an unauthenticated manner for exchanging HTTP messages. The application of unauthenticated TLS - particularly when Perfect Forward Secrecy (PFS) algorithms are used - change monitoring from being a passive attack into an active attack.

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 July 27, 2014.

Table of Contents

1. Introduction

The exchange of information through the use of Hypertext Transport Protocol (HTTP) [RFC2616] is widespread, with the vast majority of such traffic exchanged in the clear. As described in [I-D.farrell-perpass-attack], passive monitoring is seen as an attack on the privacy of users and organizations. The ubiquity of unencrypted HTTP coupled with the pervasiveness of passive monitoring means that the vast majority of HTTP traffic can be (and often is) captured without the knowledge or consent of the primary parties - namely the HTTP user agent and HTTP server - and with negligible effort on the part of the passive monitor.

Therefore, it is desirable to apply apply encryption to the HTTP exchange in the form of Transport Level Security (TLS) [RFC5246]. Traditionally, TLS has only been seen as useful if at least the

server is authenticated in the handshake, and that authentication is done almost exclusively using PKIX certificates. However, using TLS in an unauthenticated manner can mitigate passive monitoring attacks by requiring the attacker to act as a man-in-the-middle, thereby increasing the effort passive monitoring requires to be effective. Forgoing TLS authentication eliminates the burden of obtaining properly issued PKIX certificates, reducing the effort it takes to deploy an encrypted HTTP server.

1.1. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

This document reuses HTTP terminology from [RFC2616], [RFC2817], and [RFC2818]. It reuses PKIX terminology from [RFC5280] and [RFC6125].

2. How it Works

When given a "http:" URI, the user agent attempts to establish a TLS connection to the indicated origin. The exact processes used to upgrade the connection to TLS is out of scope for this document; it could use the Upgrade process documented in [RFC2817], or attempt to connect to the server on the IANA-registered port for HTTP over TLS (HTTPS) if the requested origin uses the IANA-registered port for HTTP. During the TLS establishment, the user agent and server ignore any certificate verification errors it might encounter with regards to naming (e.g., self-signed certificate, or none of the certificate identifiers not match the input URL).

Once established, the user agent and server then exchange HTTP messages as if the connection were unencrypted. The use of HTTP basic authentication is still NOT RECOMMENDED, and user agents MUST NOT indicate in any way that the HTTP connection is protected (e.g., display a "locked" or "protected" indicator with the HTTP resource).

2.1. Forward Secrecy

The benefits of unauthenticated TLS are only realized if it is less costly for an attacker to actively interject itself into the TLS session than to passively collect all traffic and later compromise the TLS handshakes. Forward secrecy prevents a passive monitor from decrypting the TLS session if it has compromised the server's private key. Software MUST use algorithms that provide perfect forward secrecy (e.g., TLS_DHE, TLS_ECDHE, or TLS_DH_anon) when relying on unauthenticated TLS.

2.2. Upgrade Failure

If the TLS connection could not be established, user agents need to determine whether to continue based on their own policies. For instance, a user agent might (among other possibilities):

1. prompt the user that communications with the server can be monitored and asking whether the user wishes to proceed anyway;

2. abandon the connection altogether, informing the user that privacy protection could not be applied to the connection; or

3. silently continue without any encryption. Note this can effectively lead to downgrade attacks.

2.3. Caching Upgrade Results

A user agent SHOULD cache the success or failure to establish a TLS connection with a given origin. How much information about a successful (or failed) attempt at establishing a TLS connection is implementation and deployment specific, but needs to at least indicate if unauthenticated TLS was used.

This cached information can then used for subsequent connections. If a previous upgrade was successful, the user agent can decide to fail if a subsequent TLS establishment fails. If a previous upgrade used a specific certificate chain, the user agent can fail if a different chain is presented.

3. Security Considerations

This entire document discusses security.

4. IANA Considerations

This document has no actions for IANA.

5. References

5.1. Normative References

[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.

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

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[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, March 2011.

5.2. Informative References

[I-D.farrell-perpass-attack] Farrell, S. and H. Tschofenig, "Pervasive Monitoring is an Attack", draft-farrell-perpass-attack-03 (work in progress), December 2013.

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

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

Author's Address

Matthew Miller
Cisco Systems, Inc.

Email: mamille2@cisco.com