

Network Working Group
Internet-Draft
Expires: January 30, 2007

T. Hardie
Qualcomm, Inc.

A Strawman proposal for HTTPS as a PIDF-LO Transport Protocol
draft-hardie-geopriv-https-strawman-00.txt

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 January 30, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes a strawman approach to using HTTP (HTTP) over TLS (TLS) with Digest Authentication to transport PIDF-LO ([RFC 4119](#)) objects. It is a GEOPRIV transport protocol as described in [section 5.2](#) or [RFC 3693](#) ([RFC 3693](#))

1. Requirements notation

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](#)].

[2.](#) Introduction

This document describes a strawman approach for HTTP to transport PIDF-LO objects. [RFC 3693, Section 5.2](#) says the following about Geopriv transport protocols:

"A protocol that just transports the LO as a string of bits, without looking at them (like an IP storage protocol could do), is not a using protocol, but only a transport protocol. Nevertheless, the entity or protocol that caused the transport protocol to move the LO is responsible for the appropriate distribution, protection, usage, retention, and storage of the LO based on the rules that apply to that LO."

While it might be possible to describe HTTP as a transport protocol and punt all of the requirements to the layer above HTTP, this document describes a layering of HTTP over TLS with Digest Authentication in use between client and server, so that a common set of mechanisms for privacy and authentication are established.

[3.](#) Applicability Statement

HTTP can be used as a substrate to a number of different applications, and defining a set of guidelines for the transport of PIDF-LO for any application which might use HTTP would be difficult or impossible. This document does not attempt that task. Instead, it is limited in applicability to the case where a client uses an HTTP GET request to retrieve a PIDF-LO object from a server or uses HTTP PUT to publish a PIDF-LO object to a server. No other functionality is covered. This document does not describe how you would determine the URI of the PIDF=LO document or the appropriate server to query.

This document does not describe HTTP as a "using protocol" which, in GeoPRIV terms, is a protocol which "uses (reads or modifies) the Location Object".

[4.](#) Steps for retrieval

[4.1](#) The client uses HTTPS to connect to the server.

The client establishes an HTTPS connection to the server, as described in [RFC 2818](#). At the TLS layer, the use of TLS_NULL_WITH_NULL_NULL MUST NOT be used as the CipherSuite.

[4.2](#) The client authenticates to the server.

The client authenticates to the server using HTTP's digest authentication mechanism as described in [RFC 2617](#) and updated

by the errata.

[4.3](#) The client retrieves the resource.

The client retrieves the PIDF-LO resource using an HTTP GET request.

[5.](#) Steps for publication.

[5.1](#) The client uses HTTPS to connect to the server.

The client establishes an HTTPS connection to the server, as described in [RFC 2818](#). At the TLS layer, the use of TLS_NULL_WITH_NULL_NULL MUST NOT be used as the CipherSuite.

[5.2](#) The client authenticates to the server.

The client authenticates to the server using HTTP's digest authentication mechanism as described in [RFC 2617](#) and updated by the errata.

[5.3](#) The client publishes the resource.

The client publishes the PIDF-LO resource using an HTTP PUT request.

[6.](#) IANA Considerations

This document does not imply any actions for IANA.

[7.](#) Security Considerations

This document presumes that the use of TLS as substrate to HTTP is sufficient to protect the privacy of the PIDF-LO content while in flight. It also presumes that Digest Authentication, combined with the TLS-layer authentication, is sufficient to enable a client and server to authenticate to one another. There is ongoing work to update Digest Authentication, and those may eventually require an update to the recommended authentication method.

[8.](#) References

(Citations incomplete; to be completed as above)

[9.1](#) Normative References

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

Levels", [RFC 2119](#), [BCP 14](#), March 1997.

- [9] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [RFC 4119](#), December 2005.

[9.2](#) Informative References

Author's Addresses

Ted Hardie
Qualcomm, Inc.
Email: hardie@qualcomm.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.