Abstract

This document defines an HTTP header field that can be added to a response to indicate to a client that a response will only be provided over a TLS connection, and only if the client has provided a certificate on that connection.

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 September 10, 2014.

Copyright Notice

Copyright (c) 2014 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 Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

Client authentication in HTTP sometimes relies on certificate-based authentication of clients in TLS. Some uses of client authentication rely on Transport Layer Security (TLS) [RFC5246] renegotiation, triggering renegotiation in response to a request for a particular resource.

HTTP/2 [I-D.ietf-httpbis-http2] forbids the use of renegotiation, except for at the very beginning of a connection. This makes addressing some client authentication use cases difficult.

This document defines a new type of authentication scheme, "ClientCertificate" for use in HTTP authentication challenges [I-D.ietf-httpbis-p7-auth]. In combination with the 401 (Unauthorized) status code, this indicates that the resource requires client authentication at the TLS layer in order to access it.

1.1. Conventions and Terminology

At times, this document falls back on shorthands for establishing interoperability requirements on implementations: the capitalized words "MUST", "SHOULD" and "MAY". These terms are defined in [RFC2119].

2. Client Certificate Challenge

A new kind of authentication scheme (auth-scheme [I-D.ietf-httpbis-p7-auth]) for the "WWW-Authenticate" and "Proxy-Authenticate" header fields is defined with the name "ClientCertificate".

A challenge with this auth-scheme does not define the use of any parameters other than "realm". Other parameters MAY be used to
provide a client with information it can use to select an appropriate certificate. Unknown parameters MUST be ignored.

This challenge cannot be satisfied by constructing an Authorization header field [I-D.ietf-httpbis-p7-auth], it can only be satisfied by making the request on a TLS connection where an appropriate certificate has been provided by the client.

A client can use this information as a trigger to open a new connection and to use client authentication on that connection. The client can use the mechanism in [I-D.thomson-tls-care] to prompt the server to request a client certificate, to avoid the problem where the server doesn’t know to make this request.

3. Security Considerations

Clients that support this authentication scheme will create a new connection each time that they see a challenge. This could be exploited in order to generate additional load in terms of connections on both server and client.

Using new connections for client authentication has additional processing costs to the client in proving access to the private keys associated with the client certificate; and to the server in proving access to the private keys associated with their certificate twice in the case that the client opts for confidentiality protection on the client certificate.

HTTP/2 [I-D.ietf-httpbis-http2] allows clients to use the same connection for multiple origins [RFC6454]. Certificate-based client authentication as defined by this specification is bound to a single origin. This could create issues whereby the security properties of a connection could become confused. Clients MUST ensure that a client-authenticated connection is only used for the origin for which it was created.

4. IANA Considerations

IANA will [has] create[d] an entry in the HTTP Authentication Scheme Registry with the following information:

ClientCertificate

RFCXXXX (this document)

This scheme does not rely on the Authorization header field.
5. Acknowledgements

Eric Rescorla helped identify the problem and formulate this mechanism. Julian Reschke hasn’t provided any contribution yet, but he will.

6. References

6.1. Normative References

[I-D.ietf-httpbis-p7-auth]


6.2. Informational References

[I-D.ietf-httpbis-http2]

[I-D.thomson-tls-care]
Thomson, M., draft-thomson-tls-care-00 (work in progress), March 2014.

Author’s Address
Martin Thomson
Mozilla
Suite 300
650 Castro Street
Mountain View, CA  94041
US

Email: martin.thomson@gmail.com