RESTful Authentication Pattern for the Hypertext Transport Protocol (HTTP)
draft-williams-http-rest-auth-01

Abstract

This document proposes a "RESTful" pattern of authentication for HTTP/1.0, 1.1, and 2.0. The existing 401 status code and WWW-Authenticate header are used to indicate that authentication is required and for negotiation purposes. The client POSTs an initial authentication message to an indicated login URI, and reply messages are returned as new representations of a session resource named by a session URI.

This approach has a number of benefits: it can be implemented with or without help from the HTTP stack, it can be universally implemented on the server side using the Common Information Gateway (CGI) and FastCGI, it results in a session Uniform Resource Identifier (URI) that can be DELETEd to logout, it is completely orthogonal to any HTTP "routers" and proxies, and it naturally (i.e., without changing HTTP) handles multi-legged authentication mechanisms.

Among other features supported are: channel binding, an optional round trip optimization for challenge/response mechanisms, some cryptographic protection options for clients that don’t use Transport Layer Security (TLS), stronger authentication of servers/services to users (where authentication mechanisms provide that) and more.

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."
1. Introduction

We propose a pattern for HTTP [RFC2616] [XXX add reference to HTTP/2.0 as well] authentication mechanisms that, by being "RESTful", obtains a number of benefits:

- compatibility with "HTTP routing" by making no assumptions that related requests are sent over the same TCP/TLS connection;
- a "session URI" results that can be used to multiplex multiple sessions onto the same TCP/TLS connections;
- a "session URI" results that can be DELETEd to effect logout;
- a "session URI" results that has better security semantics than web cookies;
- the ability to refer to multiple sessions in one request wherever such a concept might be useful;
- can be implemented by any application without changes being required to any HTTP stack;
- can be implemented by the HTTP stack;
- on the server side this can be implemented entirely via CGI and FastCGI;
- by its RESTful nature, multi-legged authentication message exchanges are naturally handled without making any changes to HTTP.

There are probably other benefits not listed above.

The rough outline of the protocol is quite simple: initial authentication messages are POSTed to an agreed-upon or indicated resource, which then results in a new resource being created with the authentication reply message as the new resource’s representation. Thereafter any additional authentication message exchanges needed (for multi-legged mechanisms) are POSTed to the new resource without a new resource being created. The resource created by the POSTing of the initial authentication mechanism identifies the resulting session, and its URI is known as the session URI. Session URIs can be used to multiplex multiple sessions over the same TCP/TLS connections, implement logout, and share sessions across multiple related servers.

Server-initiated authentication is also possible, whereby the server
sends a challenge (not much else can be sent of value in an initial authentication message from the server besides a challenge, negotiation parameters, and, perhaps, a digital signature) in 401 errors in headers. If the server gives the client has a choice of mechanisms and the client picks one where the server sent the initial authentication message, then the client consumes that message and POSTs subsequent ones to the agreed URI.

This document replaces [I-D.williams-rest-gss].
2. Conventions used in this document

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 [RFC2119].
3. Protocol

The are very few normative protocol elements here besides the outline given in Section 1. The normative protocol elements are:

- the form of the WWW-Authenticate header values for RESTauth mechanisms;
- several new headers for advertising negotiable parameters that are orthogonal to WWW-Authenticate;
- the POSTing of authentication messages from the client, with the initial client authentication message going to either a pre-agreed URI or to a URI named in the WWW-Authenticate headers;
- the creation of a session URI as a result of the initial POST, and the subsequent POSTing of any additional authentication messages to the session URI;
- the new session URI resource representation resulting from POSTs being the server’s response authentication message, if any;
- the DELETEion of session URIs as signaling logout;
- a new header for referencing session URIs in normal HTTP requests;
- the use of channel binding [RFC5056] to TLS [RFC5246] for session protection;
- the use of session keys as an option for integrity protection when TLS is not used.

3.1. Negotiable Parameters

As can be seen in the ABNF in the preceding section, the server can offer some negotiable parameters. These are:

- Mechanism names;
- Channel binding types;
- Session binding types;
- Replay protection;

Each WWW-Authenticate header value offers a single mechanism and negotiable parameters for it. The WWW-ChannelBinding-Types header allows the server to offer channel binding types.
3.1.1. Strong Binding to TLS

Strong binding to TLS is provided via channel binding [RFC5056]. When a RESTauth mechanism provides strong authentication of the service to the user, the combination of RESTauth and channel binding results in strong authentication of the server to the user even though TLS is used for session transport protection.

3.1.2. WWW-Authenticate Header Value Prefix Syntax

The ABNF for RESTauth WWW-Authenticate header values is as follows:

```
challenge           = ( "RA-" mechname SP restauth-challenge )
mechname            = TBD
restauth-challenge  = ( login-uri SP session-types SP
                    replay-prot SP *1(mech-challenge) )
login-uri           = absoluteURI
session-types       = "s=" session-type /
                    (session-type ":" session-types)
session-type        = "cookie" / "session-ID" / "MAC"
replay-prot         = "r=" ("yes" / "no")

; TODO: add production for
; mech-challenge as a base64 string
; TODO: add MAC algorithm offers for alg agility
```

Figure 1: WWW-Authenticate ABNF

For a DIGEST-like mechanism it might look like "WWW-Authenticate: RA-Digest-SHA-256 tls-server-end-point session-ID no HE4SgWGrd/3+O7t16HkusA==". For example, the mechname for the Kerberos V5 GSS-API mechanism might be "gss-krb5", and a WWW-Authenticate header value for it might look like "WWW-Authenticate: RA-gss-krb5 http://foo.example/restauth-login tls-server-end-point session-ID no".

Note that mechanisms that may be used include: GSS mechanisms, SASL mechanisms, ad-hoc mechanisms, and so on.

3.1.3. WWW-ChannelBinding-Types Header

A new header is added by which servers MUST indicate which channel binding [RFC5056] types -if any- they support for RESTauth authentication; if the server does not support channel binding then this header MUST be absent. The header is named WWW-ChannelBinding-Types. Its values are channel binding types from the channel binding type registry [RFC5929].
3.1.4. WWW-ChannelBinding-Type Header

A new header is added by which clients MUST indicate what channel binding type they used when POSTing RESTauth authentication messages, if any; if the client did not use channel binding then this header MUST be absent. The header is named WWW-ChannelBinding-Type. Its value is a channel binding type from the channel binding type registry [RFC5929].

3.1.5. WWW-SessionType Header

A new header is added by which clients MUST indicate what session binding type they choose when POSTing RESTauth authentication messages. The header is named WWW-SessionBinding-Type. Its value is a session binding type as shown in Figure 1. This header MUST be present in RESTauth authentication HTTP requests.

3.1.6. WWW-ReplayProtection Header

A new header is added by which clients MUST indicate whether they desire replay protection when POSTing RESTauth authentication messages. The header is named WWW-SessionBinding-Type. Its value is "yes" or "no" (defaults to "no" if absent) as shown in Figure 1.

Replay protection is to be used only when TLS [RFC5246] is not, and only if a session binding type of "MAC" is also requested.

3.2. Protocol Flow

RESTauth can be initiated by a client that knows a priori that it needs to or wants to use RESTauth. Servers can also tell clients that access to certain resources require authentication, possibly including RESTauth mechanisms. When the server tells the client that it must authenticate the server may also give the client an initial authentication message for one or more mechanisms.

When the client knows a priori that it must authenticate then the client MUST know the RESTauth login URI a priori as well, as well as negotiable parameters, all of which the client might know from either an application protocol specification, or from caching this information from earlier RESTauth exchanges.

The server MUST use a 401 HTTP status code and WWW-Authenticate headers to inform the client of the need to authenticate in order to access a given resource. For RESTauth mechanisms the WWW-Authenticate header values MUST conform to the ABNF given in Section 3.1.2.
To proceed the client chooses a suitable authentication mechanism (for which, presumably, it has credentials for a desired client identity), possibly a channel binding type, possibly a session type, and whether to use replay protection.

3.2.1. One Round Trip Optimization: Challenges Born in WWW-Authenticate Headers

Some mechanisms may optimize the protocol flow by allowing the server to include challenges in the 401 response’s WWW-Authenticate header values. RESTauth allows this, but this feature is OPTIONAL: it must always be possible for a client to initiate RESTauth without first obtaining a challenge in a WWW-Authenticate header value, in which case the client must incur an extra protocol leg by obtaining the challenge (if it is at all necessary) in the server’s reply to the client’s first authentication message. The reason that this optimization is optional is to allow the implementation of RESTauth mechanisms with frameworks that only support client-initiated authentication.

A challenge may consist of a nonce, some encrypted or MACed nonce, a time-stamp, and even seemingly unrelated contents such as certificates and digital signatures. The server MAY include a login URI in challenge-laden WWW-Authenticate headers where the login URI encodes secure state regarding the challenge.

3.3. Session Binding Types: Cookie, URI, and MAC

A notion of session binding type is added for binding HTTP requests to specific RESTauth login sessions. Three types are provided:

Cookies  The traditional web cookie approach to session binding;

Session URI HTTP requests carry a WWW-Session-URI header identifying the session(s) (similar to cookies, but without all the associated baggage);

MAC HTTP requests carry a WWW-Session-URI header identifying the session(s) and a WWW-Session-MAC header that carries a MAC or MACs binding the session URI(s) to the request.

3.3.1. The New WWW-Session-URI Header

A new HTTP header is added called WWW-Session-URI whose values consist of session URIs. At least one session URI MUST be included. Each session URI is an absoluteURI. Session URIs MUST NOT have unescaped commas (’,’) embedded in them. Servers MAY fail to implement support for multiple session URIs being referenced by a
single request, in which case they MUST answer with error code <TBD>. Servers MUST validate the session URI before processing the request; if the session URI is invalid the server MUST respond with a 401 (or TBD?) status code.

3.3.2. The New WWW-Session-MAC Header

[[anchor1: Describe the header, its values, algorithm agility, and what the MAC is to be taken over. Note too that this cannot apply to request contents as we have to consider chunking, and besides, a MAC of contents really has to go as a trailer, not a header.]]

3.3.3. A MAC Trailer??

[[anchor2: ... This is only needed for RESTauthTLS, which will probably not be the common mode of use for RESTauth... unless we can produce a MAC trailer extension for HTTP/2.0, in which case this may well become a common mode of RESTauth usage.]]
4. HTTP "Routing" and RESTauth

It is common to deploy HTTP services with load-balanced servers behind a load balancer and TLS concentrator. Other techniques may also result in a multiplicity of servers acting on behalf of a single service. The load balancers may even behave like routers and route HTTP requests to the same server for all requests in a single connection, or even route HTTP requests according to the verb and resource. It helps to be able to have a notion of authenticated sessions that can be referenced by all servers responding to a given service name.

The server end of a RESTauth authentication message exchange may be terminated by one server, by many servers sharing session state (via the resources named by session URIs), or by a server-side HTTP router. Once a RESTauth session is established we assume that all servers responding to the same service name will be able to access the session resource, validate session URIs, and obtain keys for computing and validating session binding MACs. Alternatively, the router may take responsibility for session binding and signal authorization information from the established session to the HTTP servers behind the router (however, we do not here specify any methods for such signaling).

By using REST for the authentication message exchange we allow this disconnection between "session" and "connection", which therefore facilitates "routing" of HTTP requests and even off-loading of authentication and/or session binding to HTTP "routers".

This approach should be flexible enough for all existing architectures for deploying HTTP services.
5. In-band HTTP Authentication Alternatives

RESTauth is "out-of-band" in the sense that the authentication messages are exchanged independently of the application’s requests for normal resources. Of course, RESTauth exchanges may well (and often will) happen in the same TCP/TLS connection as normal application requests, so RESTauth is not really out-of-band. We use "out-of-band" and "in-band" very loosely in this section.

There exist several "in-band" HTTP authentication alternatives where the authentication message exchanges happen in the context of application resources. Here the HTTP verb and resource are application-specific and have nothing to do with authentication, and the authentication messages are exchanged via HTTP request and response headers with the server responding with a 401 status code until authentication is complete.

The extant "Basic" and "DIGEST-MD5" [RFC2617] HTTP authentication methods, as well as HTTP/Negotiate [RFC4559] are "in-band" HTTP authentication methods.

In so far as an in-band authentication method results in a web cookie or session URI/ID the distinction between in-band and out-of-band is almost trivial, as described above: authentication messages in headers vs. bodies, and HTTP verb and URL. However, if in-line authentication methods are strongly tied to the TCP/TLS connections over which they were utilized then that is a big disadvantage over RESTauth: each connection requires re-authenticating, and support for HTTP routing schemes is not clear.

HTTP/Negotiate is more troublesome because historically it has required re-authentication per-HTTP request(!).

Even if the only difference between in-band and out-of-band is a trivial one, using the REST pattern means that authentication can be implemented using with no help from the HTTP stack (even though it’s desirable to have it implemented within/by the HTTP stack), whereas there may not be a way to implement in-band authentication without help from the HTTP stack for some stacks.
6. Sample/Potential RESTauth Authentication Mechanisms

Here we describe (informatively, for now) how to use or adapt a variety of authentication mechanisms, from SSHv2, IKEv2, SASL, GSS-API, and other frameworks, so as to quickly gain a set of usable mechanisms, both, specification- and implementation-wise. This section is also intended to show that adding RESTauth mechanisms is easy.

6.1. Adapting SSHv2 Authentication Mechanisms to RESTauth

SSHv2 "userauth" mechanisms [RFC4252] typically involve a digital signature (or similar) of an SSHv2 session ID. There is no such thing as an SSHv2 session ID in HTTP. A session URI cannot serve as a stand-in for an SSHv2 session ID because a) the session URI is an outcome of authentication in RESTauth, b) to prevent cut-n-paste and replay attacks the client and the server both must contribute to the entropy of the session ID that is signed by the client.

In order to adapt SSHv2 userauth methods properly (i.e., securely), we have replace the SSHv2 session ID in the to-be-signed data with a hash of the channel binding and nonces contributed by the client and the server. As an optimization the server nonce can be sent as a challenge (this saves a round trip).

6.1.1. RESTauth Mechanism Names for SSHv2 Userauth Methods

For hash agility reasons the hash function name is part of the SSHv2 RESTauth mechanism name. To avoid "multi-level negotiation" the SSHv2 userauth method name is also part of the RESTauth mechanism name.

The RESTauth mechanism name form for SSHv2 userauth methods, then, is: ssh-<SSHv2-userauth-method-name>-<hash-function-name>.

The following RESTauth mechanisms are defined here:

- ssh-publickey-SHA-256
- ssh-hostbased-SHA-256

6.1.2. Nonces

The client and the server must each contribute 128-bit nonces.
6.1.3. "Session ID"

The ssh-publickey-SHA-256 and ssh-hostbased-SHA-256 mechanisms use the following instead of a traditional SSHv2 session ID:

- SHA-256((client_nonce XOR server_nonce) || channel_binding)

Here the <channel_binding> is as per-[RFC5056]: the channel binding type name, followed by the channel binding data (e.g., ‘tls-server-end-point’ followed by the server EE certificate as sent in the server’s TLS Certificate message).

Note that use of channel binding when using SSHv2 mechanisms is REQUIRED so as to defeat cut-n-paste attacks by weakly-authenticated servers.

6.2. Adapting IKEv2 Authentication Mechanisms to RESTauth

[[anchor3: TBD.]]

6.2.1. Adapting IKEv2 Password Authenticated Connection Establishment (PACE) to RESTauth

[[anchor4: TBD.]]

6.3. Using SASL Authentication Mechanisms with RESTauth

Simple Authentication and Security Layers (SASL) [RFC4422] is a simple, pluggable framework for authentication mechanisms.

To use a SASL mechanism in RESTauth just prefix "SA-" to the SASL mechanism name and use that as the RESTauth mechanism name. If the SASL mechanism is server-initiated then the server’s challenge is sent in the server’s WWW-Authenticate header value as described above. All other SASL authentication messages are exchanged as described above (i.e., via POSTs, first to the login URI, then to the session URI, with response messages as the new representation of the session resource).

The HTTP status code functions as the application’s outcome of authentication message.

The server’s WWW-Authenticate header values function as the mechanism listing operation. SASL security considerations [RFC4422] [RFC5801] apply (particularly regarding the negotiation of channel binding).
6.3.1. Using SCRAM in RESTauth

SCRAM [RFC5802] is a DIGEST-like mechanism for SASL. Nothing special is needed to use SCRAM versus any other SASL mechanism, except for the round trip optimized form of SCRAM (see below).

6.3.2. Using SCRAM with Round Trip Optimization in RESTauth

6.4. Using GSS-API Authentication Mechanisms with RESTauth

The Generic Security Services Application Programming Interface (GSS-API) [RFC2743] is another pluggable mechanism framework. Any GSS-API mechanism that supports channel binding [RFC5056] can be used as SASL mechanisms via the "SASL/GS2" bridge [RFC5801]. This includes the Kerberos V5 GSS-API mechanism [RFC4121].
7. IANA Considerations

TBD (header registrations, ...)

Internet-Draft             RESTful Authentication             August 2012

Williams                Expires February 14, 2013              [Page 17]
8. Security Considerations

This entire document deals with security considerations. [Add more, like about channel binding, same-origin-like constraints on the login and session absolute URIs’, ...]
9. TODO

[[anchor5: Add references (to HTTP/2.0, CGI/fCGI, ...).]]

[[anchor6: Describe MAC session binding option and replay protection in detail. Describe how to extract keys for MAC keying from SASL/GSS/PACE.]]

[[anchor7: Figure out how to adapt IKEv2 password-based methods to RESTauth. This may not be worthwhile (since each method tends to depend heavily on the entire IKEv2 framework in ways that add messaging that we’d not need in RESTauth).]]
10. References

10.1. Normative References


10.2. Informative References


Connection Establishment with the Internet Key Exchange Protocol version 2 (IKEv2), RFC 6631, June 2012.


Author’s Address

Nicolas Williams
Cryptonector, LLC

Email: nico@cryptonector.com