Web Authorization Protocol WG

Hannes Tschofenig, Derek Atkins

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- 1. Agenda Bashing, WG Status
  (+ Welcome Derek and Thank You Barry)

- 2. OAuth Threats Document (Torsten)
  https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-threatmodel/

- 3. OAuth Assertions (Mike)
  https://datatracker.ietf.org/doc/draft-ietf-oauth-assertions/
  https://datatracker.ietf.org/doc/draft-ietf-oauth-saml2-bearer/
  https://datatracker.ietf.org/doc/draft-ietf-oauth-urn-sub-ns/

- 4. MAC Token (TBD)
  https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-http-mac/

- 5. Re-charter finalization (all)

  See mail sent separately to the mailing list.

Charter Proposal

Description of Working Group

The Web Authorization (OAuth) protocol allows a user to grant a third-party Web site or application access to the user's protected resources, without necessarily revealing their long-term credentials, or even their identity. For example, a photo-sharing site that supports OAuth could allow its users to use a third-party printing Web site to print their private pictures, without allowing the printing site to gain full control of the user's account and without having the user sharing his or her photo-sharing sites' long-term credential with the printing site.

Charter Proposal, cont.

The OAuth protocol suite encompasses

- a procedure for allowing a client to discover a resource server,
- a protocol for obtaining authorization tokens from an authorization server with the resource owner's consent,
- protocols for presenting these authorization tokens to protected resources for access to a resource, and
- consequently for sharing data in a security and privacy respective way.

In April 2010 the OAuth 1.0 specification, documenting pre-IETF work, was published as an informational document (RFC 5849). With the completion of OAuth 1.0 the working group started their work on OAuth 2.0 to incorporate implementation experience with version 1.0, additional use cases, and various other security, readability, and interoperability improvements. An extensive security analysis was conducted and the result is available as a stand-alone document offering guidance for audiences beyond the community of protocol implementers.

Charter Proposal, cont.

The working group also developed security schemes for presenting authorization tokens to access a protected resource. This led to the publication of the bearer token as well as the message authentication code (MAC) access authentication specification.

OAuth 2.0 added the ability to trade a SAML assertion against an OAUTH token with the SAML 2.0 bearer assertion profile. This offers interworking with existing identity management solutions, in particular SAML based deployments.

OAuth has enjoyed widespread adoption by the Internet application service provider community. To build on this success we aim for nothing more than to make OAuth the authorization framework of choice for any Internet protocol. Consequently, the ongoing standardization effort within the OAuth working group is focused on enhancing interoperability of OAuth deployments. While the core OAuth specification truly is an important building block it relies on other specifications in order to claim completeness. Luckily, these components already exist and have been deployed on the Internet. Through the IETF standards process they will be improved in quality and will undergo a rigorous review process.

Goals and Milestones

[Editor's Note: Here are the completed items.]

Done Submit 'OAuth 2.0 Threat Model and Security Considerations' as a working group item

Done Submit 'HTTP Authentication: MAC Authentication' as a working group item

Done Submit 'The OAuth 2.0 Protocol: Bearer Tokens' to the IESG for consideration as a Proposed Standard

Done Submit 'The OAuth 2.0 Authorization Protocol' to the IESG for consideration as a Proposed Standard

[Editor's Note: Finishing existing work. Double-check the proposed dates - are they realistic?]

Jun. 2012 Submit 'HTTP Authentication: MAC Authentication' to the IESG for consideration as a Proposed Standard

Apr. 2012 Submit 'SAML 2.0 Bearer Assertion Profiles for OAuth 2.0' to the IESG for consideration as a Proposed Standard

Apr. 2012 Submit 'OAuth 2.0 Assertion Profile' to the IESG for consideration as a Proposed Standard

Apr. 2012 Submit 'An IETF URN Sub-Namespace for OAuth' to the IESG for consideration as a Proposed Standard

May 2012 Submit 'OAuth 2.0 Threat Model and Security Considerations' to the IESG for consideration as an Informational RFC

New Milestones

Aug. 2012 Submit 'Token Revocation' to the IESG for consideration as a Proposed Standard

[Starting point for the work will be http://datatracker.ietf.org/doc/draft-lodderstedt-oauth-revocation/]

Nov. 2012 Submit 'JSON Web Token (JWT)' to the IESG for consideration as a Proposed Standard

[Starting point for the work will be http://tools.ietf.org/html/draft-jones-json-web-token]

Nov. 2012 Submit 'JSON Web Token (JWT) Bearer Token Profiles for OAuth 2.0' to the IESG for consideration as a Proposed Standard

[Starting point for the work will be http://tools.ietf.org/html/draft-jones-oauth-jwt-bearer]

Jan. 2013 Submit 'OAuth Dynamic Client Registration Protocol' to the IESG for consideration as a Proposed Standard

[Starting point for the work will be http://tools.ietf.org/html/draft-hardjono-oauth-dynreg]

Sep. 2012 Submit 'OAuth Use Cases' to the IESG for consideration as an Informational RFC

[Starting point for the work will be http://tools.ietf.org/html/draft-zeltsan-oauth-use-cases]