IETF Work on HTTP Authentication

Position paper for W3C Workshop on Transparency and Usability of Web Authentication, Lisa Dusseault, March 10 2006.

The IETF is working on a number of technologies related to HTTP Authentication. Some of these offer solutions to various problems or requirements. Other technologies offer use cases and possible early implementation and deployment areas.

Federated Identity

Much, though not all of the HTTP authentication work going on in the IETF, involves federated identity. To talk about that work we first need some minimal terminology and requirements or ideal properties.

Terminology: The **relying party** is usually a server and the **authenticating party** usually a client, as with today's authentication solutions. Federated identity systems add at least one new party: the **authentication provider** as a separate entity from the relying party.

Ideal Properties of a Federated Identity System

1. No need for an explicit, pre-existing business relationship between the relying party and the authentication provider, before the authenticating party attempts to authenticate.
2. Able to make assertions of facts that have an independent existence outside the assertion itself. E.g. that an authenticating party works for OSAF, is over 18, and/or lives in CA.
3. Possible to have multiple independent assertions.
4. Given that a user can demonstrate multiple assertions, the user can also demonstrate some of these assertions without revealing all of them.
5. Supports Web browsers and the existing Web infrastructure, including proxies.
6. Seamlessly supports HTTP-based rich clients (news aggregators, WebDAV, CalDAV) – these are stateless and do not use HTML forms to authenticate.
7. Supports connection-oriented clients (IMAP, POP3, FTP, SIMPLE, XMPP).

Note that properties 1 and 2 are somewhat at opposing. It's hard to know how a relying party would know whether or not the authentication provider was really able to assert that the authenticating party was over 18 years old or lived in CA.

Note that properties 5, 6 and 7 are challenging to solve together. Authentication systems that come to mind as appropriate for Web browsers are not what come to mind for smart clients, even sometimes HTTP-based smart clients (e.g. WebDAV file sharing clients).

Individuals have brought various proposals to IETF that the IETF is considering adopting and working on, and more proposals yet are expected. These include:

- DIX BOF and proposed protocol
- HTTP Claim Authentication

- Kerberos based HTTP Authentication.

Use Cases or Applications

WebDAV base and ACL

WebDAV is used to share files, backup files, and sometimes even to edit Web content.

a) Users wish to share files with users in other companies, without making those files entirely publicly-readable (properties 1 and 2)

Some WebDAV servers have implemented a stop-gap approach for this in the form of simple authorization tickets that can be passed around in email, rather than use ACLs which today only work for sharing with users on the same system.

Since WebDAV refers to principals in ACLs using URLs, this suggests a minor new required property:

9. Principal identifiers obtained from third parties can be cast to a URL.

AtomPub

There are many blogging servers, and we assume each blogger typically has an account on one home site.

b) Bloggers comment on other blogs on remote servers, and wish to associate some comments with their own blog or blogging account.

XCAP and SIMPLE

The SIMPLE WG is working on both an instant messaging protocol based on SIP, and XCAP, a way to edit and manage configuration data related to instant messaging (e.g. buddy lists, whitelists, personal contact information). XCAP uses HTTP to edit XML documents piece-wise.

c) IM users clearly need to be able to do single-sign-on to their XCAP server and their SIMPLE server. Properties 6 and 7 are required.

CalDAV

This protocol extends HTTP and WebDAV to provide calendar repository access. Calendaring involves many use cases that are interesting for authentication.

d) Information workers need to share free-busy time, and sometimes calendars, across organizational boundaries. E.g. Boeing has issued a federated free-busy challenge through The Open Group. Their challenge requires property 2 so that a user is reasonably certain they're really sharing their calendar information to a known other person they are supposed to work with.

e) Calendaring ties deeply into email with iMIP. Many email solution vendors provide calendaring as well. Single sign-on is key to those vendors' solutions interoperating with a variety of clients and that needs to work both for IMAP/POP3 and CalDAV (properties 6 and 7).

f) Scheduling and invitations workflows suggest a future need for users to identify each other directly in order to negotiate directly and choose meeting times over a live channel (property 7).

g) Calendars are often available in multiple formats: on the Web, RSS feeds, CalDAV. These should be single-sign-on (properties 5 and 6).

Summary

Although there are too many requirements here to solve them all in one specification, we need to be conscious of the needs of many applications as we make changes to HTTP authentication. Separate specifications need to be reviewed together with other pieces of a solution to make sure that implementers are able to fit together the pieces appropriately.