UMA telecon 2009-11-19

UMA telecon 2009-11-19

- Date and Time
- Attendees
- Agenda
- Minutes
  - Administrative
  - Spec progress
  - Implementation efforts
  - New Action Items
  - Scenario discussion
- Next Meeting: UMA telecon 2009-12-03

Date and Time

- Day: Thursday, 19 Nov 2009
- Time: 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
- Dial-In:
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Attendees

Voting participants:
1. Trent Adams
2. Hasan Akram
3. Paul Bryan
4. Domenico Catalano
5. Peter Davis
6. George Fletcher
7. Tom Holodnik
8. Maciej Machulak
9. Eve Maler
10. Christian Scholz

Non-voting participant:

- Jonas Hogberg

Regrets:

- Iain Henderson

Agenda

- Administrative
  - Roll call and administrative stuff
  - Approve minutes of UMA F2F 2009-11-02 and UMA telecon 2009-11-12
  - Reminder of resources linked from our home page
- Spec progress
  - Implementation review (latest work will be linked as soon as it’s available; current proposal here, and see also recent meeting notes and flows)
- Scenario discussion
  - Any new scenarios coming in soon? (Maciej, Gerry, Eve, Tom H,...?)
  - Schedule for scenario/use case review and approval
  - E-commerce scenario
- AOB

Minutes

Administrative

Roll call and administrative stuff

Quorum not reached. (Eve will do a "non-voting participant" round this week.)

- Approve minutes of UMA F2F 2009-11-02 and UMA telecon 2009-11-12

Deferred due to lack of quorum.
### Action item review

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-10-15-2</td>
<td>Eve</td>
<td>Write a &quot;Hey, Sailor&quot; scenario to illuminate the needs around Requesters that ask for resource access without the User expecting them.</td>
</tr>
<tr>
<td>2009-10-22-3</td>
<td>Christian</td>
<td>Write up a proposal as discussed on his previous call with Paul and Eve.</td>
</tr>
<tr>
<td>2009-11-02-1</td>
<td>Hasan</td>
<td>Incorporate &quot;protected status query&quot; issue into Scenarios doc.</td>
</tr>
<tr>
<td>2009-11-02-2</td>
<td>Eve</td>
<td>Start a work-item (&quot;issues&quot;) list.</td>
</tr>
</tbody>
</table>

### Reminder of resources linked from our home page

Done. Eve will will try to keep this up to date.

### Spec progress

#### Implementation review

See Paul's latest proposal and Eve's swimlane version.

All three OAuth-based flows are complete now. There's now a three-way association among the host, requester, and AM, using one three-legged OAuth instances for user/host/AM, and two two-legged OAuth instances for requester/host and requester/AM. Paul believes we'll have to truly profile/standardize on user/host/AM and requester/AM, though it will be possible to pull out and replace the mechanism we choose. But OAuth usage in requester/host is not at all mandated. We just mandate the assignment of the identifier.

The previous step 3 proposal allowed for a MITM attack, which is now mitigated.

#### Step 1:

George: Why can't metadata related to XRD-1 and XRD-2 be provided in the AM's general XRD? Paul: The semantics for authenticating at the AM as a host are different from authenticating at the AM as a requester, so there are different requirements. Maybe we could aggregate all the host-related metadata for one AM at one place, but making it possible to have different metadata per resource ("host root resource" vs. "H->A authentication descriptor") allows for more flexibility. George: But you could define some properties inside the Link element that the host needs to know. Eve: It sounds like there aren't any particular security considerations in merging them so far, but there are AM deployment expectations to consider, and also the impact on the number of steps in the protocol. George: As long as XRD-3 (host resource descriptor, specific to an individual host) is signed on its own (Paul notes that it's protected by https but he has not yet proposed that it be signed), we're okay.

George: We should document our assumption that the user has some identity at the host, and in these transactions, the host understands that identity. (Noted in spec issues list.) The host resource ultimately created at the AM is really for the "host in the context of a particular user", not just that host generically.

What are the considerations in an XRD-1+XRD-2 merge? For large AMs, it's very hard to get the e.g. AOL.com XRD to change, so pushing off some metadata to another location gives more flexibility. But you'd want the two to be linked cryptographically somehow, and you'd need to consider signing each. Do we need to consider offering both options? There might be trust-profile optimizations in the collapsed form that won't be available in the separated form. But XRD-1 is just generic information available to anybody, and doesn't seem to need special trust-profile protections. Ideally most of this stuff would be handled in libraries, so that the complexity would be invisible to implementors and deployers (though developers should still understand the underlying concepts).

#### Step 2:

This is just an example, using OAuth. It could use cookies or something instead.

George: So if the requester is representing a different user who's "behind" it each time it approaches the same host, it has to present itself differently, right? Paul: If Google approaches the resource representing itself (all of Google), the host may protest. So Google may have to establish some kind of identifier that's specific to the Google user it is representing in this instance. George: So we need to describe how the requester can implement this logic correctly. Paul: It might be in the form of a claim that says Google will use this data for the benefit of some user; indeed there is a correlation issue here. But he doesn't think Google would need to get a new access token for all its users.

Since in UMA an "access token" doesn't actually grant authorization for access, should we consider renaming it? E.g., in step 2, if Google as a requester were to get an access token, they're still pretty far away from successfully GETting the protected resource, and part of that later process might require providing more information (maybe in the form of claims) to specify the requesting user.

Tom: The AM seems to need to know the whole calling chain in order to make a decision. When the requester does a GET, how does the AM have the ability to go back to the original user who owns all this data and present the proposition to them? Paul: Yes, the resource has to be correlated with the owner, which is work in progress. Today, the referral resource provides key info to make the correlation happen across all the parties. Tom: He will overlay the emerging design on top of his use cases to see what happens. And maybe these exercises will inform the kinds of claims we'll need to recommend as a minimum set.

Not only should the spec contain a full example of anything that we consider to be required to implement (because people will tend to look only at examples), but we should also provide lots of other collateral breaking down the flows and clarifying exactly how many of the steps are one-time-only depending on who you are and what you're trying to do. Note that no part of the flow is truly optional, in that they all have to be done somehow, at least once. Even prior mutual AM-host authentication, a la OAuth as it is deployed today, doesn't allow you to skip something like the host's POSTing of the unsigned host creation request.

### New spec issues:

See Paul's latest proposal and Eve's swimlane version.
• Consider whether the contents of XRD-1 and XRD-2 should be merged somehow.
• Consider what we should say about whether XRD-3 should be signed.
• Make it clear that, just like in regular OAuth as deployed today, we assume that the same person (the person serving as the authorizing user) is "behind" both the host and the AM.
• Make it clear that, unlike in two-legged OAuth today, the requester somehow needs to present itself uniquely per requesting user.

Implementation efforts

In addition to Maciej’s Java implementation work already under way, Hasan’s group is considering doing a C# implementation. Also, Andrew Arnott (who works in Microsoft’s Visual Studio group) is interested in implementing in C#.

New Action Items

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-11-19</td>
<td>Eve</td>
<td>Work with Maciej and Hasan to produce a slide deck explaining the protocol.</td>
</tr>
<tr>
<td>2009-11-19</td>
<td>Paul</td>
<td>Flesh out the rest of the flow, including claims support.</td>
</tr>
<tr>
<td>2009-11-19</td>
<td>Eve</td>
<td>Create a Confluence document page for the UMA Core protocol.</td>
</tr>
<tr>
<td>2009-11-19</td>
<td>Eve</td>
<td>Share the latest flow and swimlane diagram with the relevant communities to get OAuth/XRD/LRDD feedback.</td>
</tr>
<tr>
<td>2009-11-19</td>
<td>Hasan</td>
<td>Reach out to Andrew Arnott to support his implementation interest.</td>
</tr>
</tbody>
</table>

Scenario discussion

• Any new scenarios coming in soon? (Maciej, Gerry, Eve, Tom H....?)
• Schedule for scenario/use case review and approval
• E-commerce scenario

Deferred.

Next Meeting: UMA telecon 2009-12-03

As previously agreed, we’ll skip 2009-11-26 because it’s the U.S. Thanksgiving holiday.

• Day: Thursday, 3 Dec 2009
• Time: 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
• Dial-In:
  • Skype: +9900827042954214
  • US: +1-201-783-9022 | Room Code: 295-4214 (other local country numbers available on request)