UMA telecon 2010-08-12

UMA telecon 2010-08-12

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-08-05 meeting
  - Action item review
  - Chair and Use Cases Editor elections
  - Status reports from the wider UMA world
  - Resource/scope registration discussion
- Next Meetings

Date and Time

- WG telecon on Thursday, 12 Aug 2010, at 9-10:30am PT (time chart)
- Skype line "C": +9900827042954214
- US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Administrative
  - IRC channel reminder: #umawg on irc.freenode.net (web interface)
  - Roll call
  - Approve minutes of 2010-08-05 meeting
  - Action item review
  - Chair and Use Cases Editor elections next week
  - Status reports from the wider UMA world
- Resource/scope registration discussion
  - Use cases and user stories (email)
  - Existing resource reg draft
  - Christian’s new scope reg draft
  - Impacts on steps 2 and 3 (latest core spec)
- AOB

Attendees

As of 11 Aug 2010, quorum is 6 of 11.

1. Adams, Trent
2. Hardjono, Thomas
3. Holodnik, Tom
4. Machulak, Maciej
5. Maler, Eve
6. Moren, Lukasz
7. Scholz, Christian

Non-voting participants:

- Mario Hoffmann
- Kevin Cox
- Herve Ganem
- Mark Lizar
- Anna Ticktin (staff)

Regrets:

- George Fletcher
- Domenico Catalano

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue</th>
<th>Open/Close</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-08-12</td>
<td>Eve</td>
<td>Open</td>
<td>Meet to discuss how to move forward on the Scenarios and Use Cases document.</td>
</tr>
<tr>
<td>2010-08-12</td>
<td>Mario</td>
<td>Open</td>
<td>Revise the Scenarios and Use Cases document by end of August.</td>
</tr>
</tbody>
</table>
Roll call

Quorum was reached.

Herve works for Gemalto. He became interested based on a recent talk on UMA given by Eve at the Cloud Identity Summit.

Approve minutes of 2010-08-05 meeting

Minutes of 2010-08-05 meeting APPROVED.

Action item review

- 2009-12-03-4 Eve Open Add terms-negotiation scenarios to Scenarios document. (This could move to Mario in future.)
- 2010-07-08-2 Christian Open Automate the process of generating viewable HTML and TXT from the xml2rfc files and put them in a consistent place. Christian has now completed this task.
- 2010-08-05-1 Eve Closed Edit draft 00 of dynamic client registration draft and submit to IETF. This was submitted and garnered some comments, which Christian has started collecting on our wiki.

This spec is now credibly implementable, but there are a number of outstanding issues. Christian has started editing our version of the spec; we should see what the OAuth group says about our request for it to become a work item, and in the meantime we can keep on editing it and produce a draft 01 at any time.

- Can Maciej run next week’s call since Eve will be attending PII 2010 next week? Yes. Eve will do the agenda.

Chair and Use Cases Editor elections

Eve has nominated herself for the Chair position again.

Mario has nominated himself for the Use Cases Editor position. He has been following the UMA work for a long time. He has been with Fraunhofer SIT for 11 years, focusing on profile management and identity management, and has been involved in research projects in these areas.

- Motion to undertake a non-secret ballot for the chair position (unanimously) APPROVED.
- Motion to approve Eve Maler as the UMA WG chair APPROVED (by acclamation).
- Motion to undertake a non-secret ballot for the use cases editor position (unanimously) APPROVED.
- Motion to approve Mario Hoffmann as the UMA WG use cases editor APPROVED (by acclamation).

We will target the end of August to do an initial revision to the Scenarios and Use Cases document.

Status reports from the wider UMA world

Published results from the SMART UX study may be available next week.

The paper that some of us submitted to the ACM DIM workshop got accepted! Maciej and possibly Eve will be in attendance.

Resource/scope registration discussion

- Use cases and user stories (email)
- Existing resource reg draft
- Christian's new scope reg draft
- Impacts on steps 2 and 3 (latest core spec)

In the SMART project context, they have learned that:

- Users logged in at a host want to click on a button next to a resource and be presented with a window where they have options for protection on that resource. As a consequence, individual resources can be protected one by one.

- Users logged in at an AM want to see all the registered applications (hosts) and be presented with all the resources at each that are candidates for protection and select among them.

These examples are about individual resources, but we anticipate that groups of resources are going to be subject to the same requirements. Eve had proposed constructing Agile-style user stories in order to get us to empathize with users in the kinds of protection they require. Trent wonders if the user stories would be completely different for different kinds of resources, since access control of highly sensitive identity data is a different proposition from access control of user-generated content. He suspects that the added value of UMA is much greater in the cases of high-value transactions (like bio-pharma use cases).

Tom observes that some types of controlled access involve static sets of requesting parties (friends and family) and other types involve attributes that the requesting parties must prove they have. So the TaxMonkey scenario might have completely different terms of access from the Flixr photo scenario. And Christian observes that different people have different “privacy personalities” that might lead them to set defaults differently.

Tom feels that the default policy idea that appears in the last user story is fundamental; that should be possible. This would seem to apply to high-value scenarios. But then other scenarios would want a default of “public”. Eve describes how her OAuth-forged connection between LinkedIn and Twitter has an interesting feature: she has configured LinkedIn to automatically replay tweets that have the “#in” hashtag in them. Can we use this method to allow users to communicate their protection desires to hosts in tagging resources managed at those hosts?
Trent notes that the protocol needs to be agnostic regarding default-open and default-closed situations. This is a valuable requirement to state in order to give assurances to those trying to solve high-value transaction problems.

Herve asks: Is it okay for a host to register only some of a user's resources for protection? Eve believes that we should preserve the option for a host, typically in consultation with a user, to register only the subset of the resources that are subject to an AM's protection. The alternative would be registering everything and then having to apply a “null policy” to those resources that should remain public. Christian wants to avoid extra protocol traffic in “null-protecting” resources. Eve also wants to preserve the option for a host to offer protection by different AMs for different resources managed by the user there.

Herve gives the example of cloud computing environments, where many people may share documents among each others. Christian suggests that host-specific defaults would be useful.

Should it be possible to UMA-protect a single resource using multiple AMs? We've discussed this in the past, and we still don't think this complexity is warranted.

Tom relates a story about a complaint someone had about blog publishing. Blog entries get posted immediately, but corrections to the post have to go into a queue for review, which is frustrating. How can corrections get propagated when they're made? This is similar to Eve's wish that Alice be able to “change resource state” on the host with the result that the new or changed resources are automatically protected under the right policy regime on the AM. This could include uploading a new photo that has the right tags (or whatever), or, Christian points out, it could include changing the metadata on an existing photo.

Mark asks: What should our model be, such that the host doesn't have to immediately tell the AM of every change as Alice makes it? This sounds too chatty. Christian's scope proposal actually avoids the host having to push full catalogs of protected resources, so this problem could hopefully be neatly avoided in that solution.

We then discussed Christian's new scope proposal in detail. It covers only the Step 1 implications, not the Step 2 (access token issuing) implications; Eve notes that this proposal therefore isn't “complete” so it can't be treated as a module in its current form. It would have to be incorporated into the core spec if we were to accept this proposal/general direction.

We have a number of big philosophical questions surrounding this whole topic:

- Should we be focusing on informing the AM about only resources, or whole scopes (resources + actions), or some other subset?
- What is the right dividing line between the AM's responsibilities and host's responsibilities?
- What are the right junctures at which we should have communications happen between the host and the AM?
- What user stories/user interaction wishes should be solved for?

We'll assess the different proposals on these bases next week.

**Next Meetings**

- WG telecon on Thursday, 12 Aug 2010, at 9-10:30am PT (time chart) on line C
- WG telecon on Thursday, 19 Aug 2010, at 9-10:30am PT (time chart) on line C
- Legal subteam telecon on Wednesday, 25 Aug 2010, at 8-9am PT (time chart) on line C