UMA telecon 2010-04-01

UMA telecon 2010-04-01

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-03-25 meeting
  - Action item review
  - Other administrative topics
  - Trusted discovery, generically and in the hData case
  - Implementation activity roundup
  - Lexicon review and prep for TomS call at noon PT
  - Signed messages issue
  - Token validation issue
  - Next Meeting: UMA telecon 2010-04-08

Date and Time

- **Day:** Thursday, 1 Apr 2010 (no, really)
- **Time:** 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC ([time chart](#))
- **Dial-in:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Agenda

- Roll call
- Approve minutes of 2010-03-25 meeting
- Action item review
  - Scenario doc refresh activity
  - Implementation activity roundup
    - Demo targets?
    - Dev list?
  - Lexicon review and prep for TomS call at noon PT
    - What to do with the legal discussion: new document?
    - Any UMAntarian can join TomS call; contact Eve for dial-in
  - Protocol issues as discussed on list
    - Token validation
    - Identity tokens
    - Any others
- AOB

Attendees

1. Adams, Trent
2. Holodnik, Tom
3. Machulak, Maciej
4. Maler, Eve

Non-voting participants:

- Gerry Gebel
- Mark Lizar
- Thomas Hardjono

Guests:

- Joni Brennan (staff)

Regrets:

- Domenico Catalano
- Brian Armstrong

Minutes

**New AI summary**

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-04-01</td>
<td>Eve</td>
<td>Open</td>
</tr>
</tbody>
</table>
Roll call
Quorum was not reached.

Gerry is formerly of Burton Group and is now with Axiomatics, an XACML-based authorization vendor. His interest is in the AM part of UMA. Thomas is from the MIT Kerberos Consortium, and his interest is in "bringing Kerberos to the web", so that enterprises can expand their web capability.

Approve minutes of 2010-03-25 meeting
Deferred due to lack of quorum.

Action item review
- 2009-12-03-04 Eve Open Add terms-negotiation scenarios to Scenarios document.
- 2010-03-10-2 Maciej Open Do next round of spec editing.
- 2010-03-10-6 Joe Open Revise the protected inbox scenario for next week's call.
- 2010-03-10-8 Eve Closed Analyze the old location scenario for suitability in documenting the "all photos in this set" scenario. Done; she thinks we still need "location" for its read/write scope properties, but also need the "photo" one for its dynamic scope properties. TomH thinks one of his scenarios might exercise this distinctive aspect ("all employees in this company").
- 2010-03-18-3 TomH Open Flesh out the small-business scenarios, including any distinctive aspects around claims etc. This is under way.
- 2010-03-25-1 Paul Open Send email giving examples of how a resource-oriented scope approach is necessary. Under way by Paul and Tom.
- 2010-03-25-2 Eve Closed Add security consideration section to the spec with a placeholder for the "TurboTax use case".
- 2010-03-25-3 Eve Closed Create fresh protocol issues list based on 2010-03-25 agenda items.

Other administrative topics
- Eve has reviewed the entire Scenarios doc and will hand out AIs for lexicon/substantive "rationalization".
- Publication of Newcastle University tech report: User-Managed Access to Web Resources – Recall that several of us wrote a paper that we submitted to the Web 2.0 Security and Privacy workshop. We don't know if our paper has been accepted yet, but we have the ability to publish it ahead of time, so we have.

Trusted discovery, generically and in the hData case
In the process of defining UMA on WRAP->OAuth 2.0, it turns out we have sort of defined a generic version of the "host/requester registration at AM /discovery service" pattern shown in the hData scenario! Eve asks whether we've got a generic resource discovery pattern here that should be recognized as such (alongside "Data Dominatrix" and "Hey, Sailor"). TomH comments that this question has come up in his small-business scenario work, and it relates to the need for a user to pre-define scope parameters so that requesters could usefully get pre-authorized directly at the AM and get a token that they can use at the host.

In UMA's olden days (using the OAuth 1.0 paradigm), we had talked about pre-authorizing requesters but not pre-provisioning them with an access token. However, once we moved onto the WRAP paradigm, those could amount to the same thing, and we had already allowed for the possibility that the requester can proceed directly to the AM if it knows the right endpoint without hitting the protected resource at the host first. We need to think about this more.

TomH also wants to be able to have the AM dynamically discover all the relevant protected resources at the host. There are actually several different kinds of discovery that are interesting:

- The AM needs to know certain things about the host and its resources
- The host needs to be introduced to the AM
- The requester needs to know what AM endpoint to go to to get a desired resource
- The requester needs to know what resources it can get
- (and there's probably more)

Mark observes that in many of these cases, often a single application will serve as both a host and a requester for different purposes. If there's a network of applications that are all hosts and requesters with each other, the AM provides a trust model in the middle to make sense of the problem of this complex "graph". It's the Borg collective, with the Borg Queen (the AM) and Locutus (a discovery service). 😝

Implementation activity roundup
Maciej reports that his Newcastle University project to do a Java-based UMA implementation now has a developer on board. They plan to build a demo AM for IIW, along with sample web applications that can function as host and requester. In addition, Paul is working on a host implementation and Domenico is making progress on some user experience design work. So all these efforts may not merge perfectly for IIW, but at the least we should be able to demo multiple independently developed host apps against at least one AM app, and to show at least mockups of some high-quality UX. And we can show all the work in progress for EIC.

Eve makes a plea for all developers to start using the Uma-dev list!

OAuth 2.0 progress: Eran H-L has begun publishing drafts of his spec.

Lexicon review and prep for TomS call at noon PT
The (wonderful) diagram from Domenico on the Lexicon page shows how Alice herself might be "behind" two different patterns of sharing/access; the protocol is the same in both cases, but the legal implications differ. If we have a goal of empowering users, does one pattern get us closer than the other?

TomH's scenarios might involve a company on the left side, albeit possibly a small businessperson who is in business for themselves. And Thomas points out that a person logged into their sole-proprietor landscaping business account is still a person who is "behind" the real authorizing party! This would make the matrix much more symmetrical, at the cost of still more complexity.

The "authorizing party" is a continuum, where it could be a person acting on their own behalf on the Web (our stated UMA 1.0 scope), a person running their own company, or a policy administrator at a company. How far should we go? Mark suggests that a separate diagram drill down into this level of detail. Eve notes that we should be careful about scope creep.

What should we do with this lexicon discussion content? We could turn it into a working draft of a technical report. Thomas spoke in favor. Eve mentioned OpenID CX as the only other effort she knows that deals with the enforceability question, though they are more comfortable "throwing crypto at the problem" (mutual digital signing of the agreement) than we are.

Signed messages issue

Paul made the case on the list that having the requester sign messages when it approaches the host is not worth the effort. It adds little in the way of basic security (though it does protect better against replay of messages), it adds complexity, and the AM is the final arbiter of the requestor's identity and whether it should have an access token anyway. TomH's concern is that non-idempotent actions taken when a requester accesses a protected resource at a host are high-value and high-sensitivity, and he may be interested in extra "are you sure?" types of protections. E.g., what if the requester is a robot that deletes every employee from the payroll (involving the "dynamic scope" requirement where the scope is all employees who are currently in the employee directory)?

Having something in the request that uniquely identifies it could protect against various types of errors. Eve notes that this would amount to a nonce, which could be helpful against replay, but then again we were intending that the same access token could be reused (a) over a short period of time and (b) against a "large" scope that includes multiple resources, multiple methods, or both.

Another scenario might involve payroll payments from a particular funding source to all employees. What happens if the funding source needs to be changed? Eve cautions that we want to ensure that we don't preclude obvious ways to solve this, but again, some of the small-business scenarios may end up being deferred for 1.0.

Our question is whether we think UMA needs to take advantage of OAuth's offering of signed messages, or not, or need to ask for some other solution at the OAuth level. TomH's further scenario work will continue to flesh this out.

Token validation issue

Maciej started this discussion on the list. If the token has structure, the host could validate it locally (having been provisioned earlier with a means for this). Or the host could validate an opaque token in real time. TomH wonders if a token could have a "watermark" which gives the host the ability to validate just the syntax ("this came from the right AM") if not the semantics. A digital signature would meet this goal, but maybe a hash would be a lighter-weight alternative.

As opposed to the "signed messages" discussion above, this subject touches on "signed tokens". Tokens need to be secure in transit, authenticated as having come from the AM, and able to be interpreted correctly by the host. What is the right mix of solutions for this? We understand the problem better now, but aren't sure of the solution yet.

Next Meeting: UMA telecon 2010-04-08

- **Day:** Thursday, 8 Apr 2010
- **Time:** 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC (time chart)
- **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)