UMA telecon 2009-09-10

Date and Time
- **Day:** Thursday, 10 Sep 2009
- **Time:** 9:10-10:30am PDT | 12:10-1:30pm EDT | 16:10-17:30 UTC (time chart)
- **Dial-In:** +1-218-862-7200 or +1-712-432-3100 (if one doesn't work, try the other)
- **Code:** 987-632 (do not press #)

Attendees
1. Andrieu, Joe
2. Bryan, Paul
3. Catalano, Domenico
4. Fletcher, George
5. Hanson, Michael
6. Machulak, Maciej
7. Maler, Eve
8. Stollman, Jeff

Regrets
- Diego Lopez
- Hasan Akram (possibly)
- Iain Henderson

Agenda
Tentatively:
- Roll call
  - If quorum: consider accepting previous Aug/Sep minutes
- Meeting schedule for the next couple of weeks
- Action item review
- Quick review/discussion of OAuth news
  - OAuth recursive delegation
- Discuss technical spec status (Paul)
- Discuss scenarios
  - Prioritize the scenario roundup
  - Discuss top two A-priority scenarios
  - If quorum: consider formally accepting Calendar scenario
- AOB

Minutes

**Roll call**

Quorum reached.

Christian was unable to get on the call successfully. He is looking into the conferencing option that DataPortability uses (which is for pay, but isn't hugely expensive). Paul is looking into setting up a SIP-based server for our own use. Gizmo is one company that provides a variety of client options for SIP, including a bridge over to Skype.

- If quorum: consider accepting previous Aug/Sep minutes

UMA telecon 2009-09-03 minutes APPROVED by unanimous consent.
UMA telecons for all of August APPROVED by unanimous consent.

**Meeting schedule for the next couple of weeks**

Eve, Jeff, and Joe will try to put their heads together briefly at the F2F opportunity, and maybe rope in Iain. But we won't consider this a formal meeting. We will meet at our usual Thursday time (Sep 17 telecon) by phone. Paul, as Vice-Chair, will run the Sep 24 telecon since Eve is unavailable.

**Action item review**

Quick review/discussion of OAuth news

- OAuth recursive delegation spec
None of us on the call have had a chance to read it thoroughly. Michael is reaching out to Eran later today about OAuth matters in general, and will take the opportunity to figure out how much UMA might be on his/OAuth’s radar. We hope to avoid unnecessary deviations where we’re trying to do the same thing.

At a quick glance, George thinks this spec seems to define a Content Manager or First Client that sounds very close to Christian’s conception of multi-resource authorization and having a service catalog. The First Client sounds like a Host, and the Second Client sounds like our Requester. Diego had wondered in email if the First Client could be, instead of a Host (in our terms), an AM (again in our terms). This spec invokes the notion of “proxying” and of temporary credentials, which is very much like our assignment of a correlation handle to the Requester. Section 3.3 has a flow diagram.

Some of the mechanisms defined do seem to be somewhat similar to the ProtectServe sketch, except that:

- It doesn’t externalize the authorization decision.
- It doesn’t have the terms offer/acceptance cycle.
- No User Agent appears in the picture; it’s not “user-driven” or “user-managed” in any sense, and chaining all the delegations forward happens on a back channel. (This is similar to many ID-WSF and VRM scenarios, except that the latter two usually presume user consent at a minimum.)

This last item could be a little scary without a notion of delegation scoping; there’s potentially the Confused Deputy vulnerability where you work through a party who has more access rights than you do in order to get stuff you don’t deserve. Also, it’s scary if the user can’t (a) audit what happened, and (b) give approval out-of-band in the fashion imagined by ProtectServe. Will users who use services that are both OAuth-enabled and “Recursive Delegation” enabled now have to opt in to a setting that says “Don’t do recursive delegation”?

There is perhaps a bit of overlap between the recursive delegation scenario and our idea for a scenario (not yet written) where the Host has to merely give the AM an audit trail of accesses that it allowed.

We’d like to engage folks on the OAuth list about these comments and ideas, and this can help get UMA some notice there. We’ll take this notion to our own list for discussion.

**Discuss technical spec status (Paul)**

Paul has just arrived back from vacation. He plans to start on a strawman spec immediately, starting with the ProtectServe point and moving from there based on discussion and scenario acceptance.

Earlier today, Paul, Christian, and Eve walked through the ProtectServe flows again and discussed rationales for their particular shape. E.g., one objective was that Hosts (SPs) should not be able to correlate Requester (Consumer) identifiers that could tie resources to the same user, which led to our notion of a Host (SP) handle. So a Requester (Consumer) key would be specific to the AM, and the Host (SP) couldn’t tell what Requesters (Consumers) a particular human being had chosen to use. This led to our deviating from canonical OAuth flows in Step 1 (even though Step 0 is essentially pure, if decorated, OAuth).

Christian’s 4-legged design chains pure OAuth multiple times, and requires the user to be present to introduce all the parties. This has Paul thinking that we can use OAuth in the process where a user authorizes a resource access “live” (Michael notes that this is a callback-like approach); currently this part of the ProtectServe design hadn’t been completed anyway. The AM could be the User Agent in this circumstance.

This approach would ramp up the complexity of the overall protocol, though – perhaps too much. And the UX might really get degraded and get more susceptible to phishing.

Michael wonders if we can avoid adding crypto requirements beyond what existing web app implementations do today; there was general agreement.

**Emergent design principle:** We should avoid adding crypto burdens as part of our simplicity goal.

**Discuss scenarios**

Motion to accept the Calendar scenario APPROVED by unanimous consent.

- Prioritize the scenario roundup and work on the top-priority scenarios

The five that are actually on the wiki get priority by being the most complete. The Calendar, E-Commerce, and Loan Request scenarios are related in the sense that they cover a single resource, multiple resources on a single Host, and multiple resources on multiple Hosts. We should probably consider these in the context of each other.

**All:** Eve: Open: Edit the E-Commerce scenario to make clear that the first written bit is about the problem space, not the solution space.

Joe mentions Scanaroo, which is an iPhone product that lets you scan in your loyalty card into your phone and then give the cashier your phone to scan in your card.

Michael notes that discovery is a constant theme, and it comes up in several places. Do we have to solve it, or can we stay away from it? Paul feels that we should avoid requiring a service catalog/discovery service. Eve has been imagining that we would rely on relationship managers that *statically* package up (on a user’s instructions) a whole series of resources (perhaps on a variety of different Hosts) into a manifest (which could be an Atom feed?); a Requester would have to first get authorization to access the manifest, and then get authorization to access each referenced resource in turn.

Joe asks if the claims are unary or use binary logic. Michael suggests that higher-level policy modeling is out of scope, but we’ll have to have primitives for handling policy and terms. A naive protocol implementation might be too chatty for real-world use, but naive implementations aren’t our concern. Paul notes that policy can be applied unilaterally – “silently” with respect to the protocol – but terms must be accounted for in the workings of the protocol somehow.

**Next Meetings**

UMA meet-and-greet 2009-09-15
We will hold a meet-and-greet for any UMA participants and lurkers at the Kantara meeting on Tuesday, Sep 15. See the Meetings and Minutes page for more details.

**UMA telecon 2009-09-17**

Our next telecon after Sep 10 will be on Sep 17.

- **Day**: Thursday, 17 Sep 2009
- **Time**: 9:10-10:30am PDT | 12:10-1:30pm EDT | 16:10-17:30 UTC ([time chart](#))
- **Dial-In**: +1-218-862-7200 or +1-712-432-3100 (if one doesn't work, try the other)
- **Code**: 987-632 (do not press #)