UMA telecon 2017-12-21

Date and Time

- Thursdays 9am PT
  - Screenshare and dial-in: http://join.me/findthomas (WILL CHANGE IN 2018)
  - UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2017-12-14
- Meeting schedule
  - No meetings next week
  - New GoToMeeting usage in the new year
  - New calendar entries in the new year – please subscribe to the calendar
  - Prepare for Roadmap discussions (see blog post here)
- Discuss security attacks and outcomes
  - 2017-12-14
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2017-12-14: APPROVED by unanimous consent.

Meeting schedule

- No meetings next week
- New GoToMeeting usage in the new year
- New calendar entries in the new year – please subscribe to the calendar
- Prepare for Roadmap discussions (see blog post here)

Eve will specifically invite voting participants to the new calendar entry, and anyone else who asks.

The first WG meeting in the new year will be on Jan 4, and the first Legal meeting will be on Jan 5.

Andi reminder: The Identiverse CfP is still open until Jan 15! Don't forget!

Discuss security attacks and outcomes

The UMA multi-endpoint mix-up attack analysis is here. Nat wrote:

(1) How does the client obtain the issuer string to bootstrap? [attack surface 1] – there are real examples for this kind of attack being successful.

(2) Has the DNS spoofing against the client for issuer combined with falsely issued certificate been considered? [attack surface 2] – there has been a real attack like this.

(3) What kind of agent a typical RqP using? If it is a browser, then browser infection to rewrite the request/response is possible. [attack surface 3] – this is a rather common attack.

It really depends on the answer, but unless there are specific considerations to block the surface, the answers to the questions “Can attacker inject false claims interaction endpoint” and “Does attacker receive claims redirection URI” seem to be both YES to me.

If No. 1 is a point of attack, then the RS is the attacker, and it has much greater/sooner opportunities for attack, as you point out in a way with the as_uri observation. We have analyzed these here. Given the potential scope of damage but also the RS's need for a relationship, we've dubbed them “trust attacks”, and they don't seem to have practical technical mitigations.

Regarding No. 2, UMA already adopts OAuth's security considerations and TLS usage and is simply defined as an OAuth grant (and FedAuthz requires TLS usage). Our thinking is that there’s no need for us to add a specific security consideration around this because there's nothing in UMA that's unique relative to OAuth (or even other TLS-using protocols).

Regarding No. 3, UMA works with clients of both public and confidential types (Grant Sec 3.3). Different security levels can thus be achieved in UMA, a bit similarly to choosing different grants in base OAuth. The browser environment obviously raises the possibility of various attacks, which is why there is so much effort in the OAuth security considerations put into that environment. The same security considerations apply.
We have consensus on these issues. We will seek a meeting with Nat to try and align on these important topics (as soon as practicable in January) and close the loop firmly. It would be great if Justin could join too. Happy holidays and happy new year to everyone!

**Attendees**

As of 7 Mar 2017, quorum is 4 of 7. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Sal
3. Andi
4. Eve
5. Mike

Non-voting participants:

- George