Henry Story <henry.story@bblfish.net>
To: Ben Laurie <benl@google.com>
Cc: public-webid@w3.org
Bcc: Adeline Gasnier <adeliga@hotmail.com>
27 September 2012 21:09

privacy definitions -- was: WebID questions

I think we have a problem with divergent understandings of what privacy amounts to,
and we should clarify this divergence. More below.

On 27 Sep 2012, at 14:45, Ben Laurie <benl@google.com> wrote:

> On 27 September 2012 13:11, Henry Story <henry.story@bblfish.net> wrote:
>
> On 27 Sep 2012, at 13:10, Ben Laurie <benl@google.com> wrote:
>
> > On 27 September 2012 12:01, Henry Story <henry.story@bblfish.net> wrote:
> > I forgot to reply to this comment:
> >
> > On 27 Sep 2012, at 12:13, Ben Laurie <benl@google.com> wrote:
> >
> > > The W3C does not seem to agree -
> > > http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html claims
> > > that some people do not want to be correlated across sites.
> >
> > Yes. We are not saying they MUST be correlated across sites, and we are not
> > removing the freedom of people who wish not to be correlated.
> >
> > When I go to a web site I don't have to click the login button. f I click
> > the login button and it asks me for a certificate I don't have to choose one
> > with a WebID - or choose one at all for that matter.
> >
> > The browser UI people could add a field in the certificate login selection
> > box for an origin-bound-certificate perhaps. I am not sure how they should
> > present this, nor what the advantages or disadvanteges of doing that would
> > be, and it is outside the scope of the discussion here.
> >
> > But if I want to login with an identity I have on the web, and I want this
> > to be correlated, then I don't see why that freedom should not be available
> > to me.
> >
> > I am just saying that practically most people will not want to have 10000
> > identities. Certainly if we restrict ourselves to identities that they want
> > to use for correlation, it seems unlikely that people can cope with more
> > than a handful or find it useful.
> >
> > I find a standard that is not interested in helping people who want to
> > log in _and_ have privacy to not be very interesting.
>
> That is stated so generally it is difficult to make much of it. You seem to want Origin-bound-certificates
> it seems as described here:
>
> http://tools.ietf.org/agenda/81/slides/tls-1.pdf
>
> (though the criticism of TLS certificates on slide 3 is wrong as I have already explained in
> http://lists.w3.org/Archives/Public/public-webid/2012Sep/0093.html)
>
> I pointed out in my reply above that perhaps origin bound certificates could be tied into a user
> experience with normal browsers and normal certificates. I don't see why there should be a standard that
> solves both problems, or why they could not work together.
>
> Now this still leaves you with the option of thinking that the problem you really care about - secure login
> to one site - is the one and only truly honest problem that an engineer needs to solve who is concerned
> about privacy. Let me spend a little time disabusing you of that understandably simple and appealing idea.
> Consider:
>

> 1. What kind of privacy do you get if you log into one site (say with Origin-bound certificates) and it offers everything to you: your social networks, your films, your news, your search, etc... Is that really privacy?
>
> 2. What incentive do you have when you go to a different site, and you log in there completely fresh? Let us imagine that that is the only thing you CAN do when you login to a new site: perhaps linked data and WebID have been made illegal in this world. So you arrive at this new site, and the number of people you can interact with is inevitably less than on mega-co's servers. You may find that cool. But where do you think the rest of humanity is going to end up on? And what does that do to your privacy when they tweet more and more where they saw you, what you told them, and in any case all the communication you send them has to go through megaco's servers.
>
> So consider why and how you came to think that "login and privacy" were the only thing to merit your attention. Also consider why you think that login and identity don't equal privacy. Say you have a freedom box and I have mine, and I go to your server and authenticate and post a picture. The only two people who can see the picture are you and me. Where is there a privacy gap there?
>
> I believe you are serious in your desire for privacy. And I respect that. But I think by not taking into account the network effect, by not noticing the many folded nature of reality, you end up working against your own values, and discarding solutions that could help you achieve your aims. So I do urge you to consider WebID as another tool to help create a more just and less asymetric space for us to live in, where we can all enjoy greater privacy and security.

> I've talked about many issues with WebID, why do you think privacy is
> my sole concern?

You said "I find a standard that is not interested in helping people who want to log in _and_ have privacy to not be very interesting." But why would you think that WebID does not enable privacy?

I then put that together with your earlier statement "that some people do not want to be correlated across sites."
Referring to a document on DO-NOT-TRACK by the W3C. It seems that you think that being correlated across sites (in any way) is a privacy problem.

If I put these together then it seems to me that you are thinking that a fundamental requirement for privacy is that one not be identified across sites in any way. You seem to exclude the possibility that I wilfully be identifying myself across a site, as one that cannot be privacy enhancing. Or else why would you think that WebID cannot be an option for people who are keen on privacy?

My understanding of privacy starts from a different intuition. A communication between two people is private if the only people who have access to the communication are the two people in question. One can easily generalise to groups: a conversation between groups of people is private (to the group) if the only people who can participate/read the information are members of that group....

So now imagine that you and I and each member of this mailing list have their own freedom box [1] . A freedom box is a one person server that serves only the person in question. I am purposefully taking an extreme example to make the point. Now lets imagine you put a picture of our future meeting at TPAC in late October - I hope you will be able to come - onto your freedom box, and tag the people who appear in that picture taken later at night in a bar. You may not want to make it public until and unless all the members who have appeared in the picture accept that picture to be public. So to keep it close to our current technology, let us say you send them an e-mail with the link to the page containing the pictures. You don't want all the people on the web who see that URL as it passes unencrypted through the etherspace to be able to also click on the URL and see the picture. So you add an access control rule to your page that only allows the people who were designed in the picture - by WebID - to access to those resources. On receiving the mail the tagged people can click on the picture's URL, authenticate with WebID, and see the picture. Anybody else who tried would not be able to see it: 403 Access Forbidden. Now I would say that those pictures are protected for privacy - they are not public, and only visible to the designated group - and you have used WebID in the process of making sure they were kept private. There was no third person in the loop that also saw the pictures. Only those people you wanted to could see them.

> My point was this: if your response to a desire for privacy _amongst
> many other things_ is "then don't use WebID" that seems like a
> deficiency in WebID to me, and one that makes it a lot less
> interesting to me.

I was only saying: if you want to log into a site without using a WebID based certificate, then don't use a WebID based certificate. But don't think that by doing that you are guaranteeing your privacy. As I explained if there is only one big web site to rule them all and you log into it without webid, whatever you post there will be seen not only by the people you wanted to have it visible to, but also by the owners of the site. In our Freedbom Box scenario that is not the case. So this is a case of showing how having a global identity that the user can control enhances privacy.

Henry

[1] http://freedomboxfoundation.org/
[2] http://www.w3.org/2012/10/TPAC/