

Henry Story <henry.story@bblfish.net>
Resent-From: Henry Story <henry.story@bblfish.net>
Resent-To: Adeline Gasnier <adeliga@hotmail.com>
To: Ben Laurie <benl@google.com>
Cc: "Jonas Hogberg K.O" <jonas.k.o.hogberg@ericsson.com>, Carvalho Melvin <melvincarvalho@gmail.com>, "public-philoweb@w3.org" <public-philoweb@w3.org>, "public-webid@w3.org" <public-webid@w3.org>, Oshani Seneviratne <oshani@mit.edu>
Re: privacy definitions -- was: WebID questions

1 October 2012 15:07



On 1 Oct 2012, at 14:35, Ben Laurie <benl@google.com> wrote:

On 1 October 2012 13:20, Henry Story <henry.story@bblfish.net> wrote:

On 1 Oct 2012, at 13:43, Ben Laurie <benl@google.com> wrote:

On 30 September 2012 20:22, Henry Story <henry.story@bblfish.net> wrote:

On 30 Sep 2012, at 20:46, Ben Laurie <benl@google.com> wrote:

On 30 September 2012 10:30, Henry Story <henry.story@bblfish.net> wrote:

On 29 Sep 2012, at 19:50, Ben Laurie <benl@google.com> wrote:

On 28 September 2012 15:26, Jonas Hogberg K.O
<jonas.k.o.hogberg@ericsson.com> wrote:

At

http://blogs.kuppingercole.com/kearns/2012/09/25/in-search-of-privacy/?goback=.gde_3480266_member_168314336,
Dave Kearns writes:

There is indeed a lot of confusion about the subject, but there are two key phrases to remember when talking about privacy:

Privacy is not anonymity
Privacy is not secrecy

Quoting those out of context is not particularly helpful. But for more on why anonymity is important for privacy...

<http://www.links.org/?p=123>

<http://www.links.org/?p=124>

Looking at those two, can we agree that we agree that anonymity should be the default? I believe as you do that when I go to a web site the default should be that I not be identified, and not be tracked. I can choose later to be tracked or identified for that site for a given amount of time or until I change my mind, but the default should be anonymity.

(Within limits of logic of course. If I tell anonymous Y something P which has consequence Q, and some other anonymous Z does something with Q that would have been nearly impossible to know had they not known P, then I could conclude within a certain probability that $Y = Z$)

The web provides this. Some browsers provide it better than others, but really this is up to them. It is not perfect: ip addresses can be tracked and dns lookups can be tracked. But the web is not reliant on those. It could be deployed just as well on top of Tor. Had people had better memories, we could have had .onion urls plastered on bus stops since the beginning.

Anonymity is important for many reasons. Among which is that it helps create a trusted public sphere. It increases my trust in the information I read if I know that the publisher publishes that information that can be read by anonymous readers. Knowing that the publisher cannot tell who is reading what he is publishing is a very strong guarantee that he is not adapting his message to different groups. Oddly enough anonymity has an important role therefore in public discussion.

So do we agree here? I think we do.

So far.

ok. So let's see if we can agree further, from here :-)

There are a number of identification options available.
Let me list some of them:

- anonymous (\emptyset identification)
- cookies (site bound)
- TLS-Origin-Bound-Certificates (unforgeable cookies)
- Self-Signed certificates with an .onion WebID
(I promised Appelbaum to work on that. This gives you an identity, but nobody knows where you or your server are located)
- Self-Signed certificates with a http(s) WebID
- CA Signed Certificates
- DNSSEC Signed Certificates
- ...?

We agree that anonymous should be the default.

I think we can agree as a matter of simple fact that none of the browsers show you which of those modes you are in when looking at a web page. You cannot as a user therefore tell if you are anonymous or not. You cannot therefore tell if the page you are looking at has been tweaked for you or if it would appear differently to someone else in the same mode as you. You cannot tell if the agent on the other side can tie you to a browsing history or not.

Well let me put this in a more nuanced way: you can tell the above from the side-effects - say if they should you your profile on a google+ page with edit mode allowed - but that is up to the server to show you that. We both want it to be up to the user. We don't want it to be up to the user in some complicated conf file hidden away somewhere. We both want it to be in your face, transparent. I should in an eyeblink be able to tell if I am anonymous or not, and I should be able to switch from one mode to the next if and when I want to in a simple easy gesture.

Just as in real life when we put on a mask we know that we are wearing the mask, so on the web we want to know what mask we are wearing at all times.

These are the improvements I have been fighting (not alone) to get browsers to implement. Are we fighting on the same side here?

I agree that it is desirable to know how your browser is identifying you and to be able to switch between users. So, I guess Chrome would claim that the facility to have multiple users provides this. Do you disagree?

I looked up multiple Users and found this:

<http://support.google.com/chrome/bin/answer.py?hl=en&answer=2364824>

I had not seen this before.

So it seems to work for certificates. I created a new user Tester, and noticed the following as that Tester:

0. It did not have any of my bookmarks (I suppose that's useful, cause your bookmarks could identify you)

1. When I went to Google+ it did not know I was

2. Having signed in to <https://my-profile.eu/> as the old user, I tried as the new user Tester, and had to select a certificate again. Good.

So that seems like one way to separate one's personalities. I'd still like to have the url bar show me for each tab:

[anonymous] when I am not logged in
[cookie] when I am tracked on that site
[henry story] for a local site identity
[bblfish@home] when I am using a certificate

With the option of logging out from that site (ie checking x -> anonymous). Because currently I could forget that I had chosen a certificate on a site, and it would continue sending it. Or I could mistakenly choose a certificate as one user, and then decide that was the wrong user for that persona, and not be able to choose the certificate again, without closing my browser completely. That would allow, on browser startup, the browser to remember the last identity choice for a site. Without logout capability that is not possible, because then it would be impossible to repair an identity mistake without creating a new user. (And it makes testing tedious).

Currently when I close my browser, on restart the servers ask me for my certificate again.

So it looks like this is going generally in the right direction. It still does not provide the transparency we are looking for at the UI level above. But thanks for pointing this out.

So I think we agree that what is missing is the transparency at the UI level of which identity one is using at each site. That is what I was hoping the following bug report would achieve.

<http://code.google.com/p/chromium/issues/detail?id=29784>

So perhaps by putting this forward under the term transparency, that would help that bug report progress, since otherwise they could think that the issue had already been completely solved.

So that's what I make of that. But have I missed something? Or do we agree there too?

I don't think so

. As I said, I think that Chrome would claim that the users facility provides everything you need - if you want to know which cert you're using, then have a user per cert. As for cookies and "local site identities", this would require information the browser does not currently have, so I think you would first have to explain how it is going to get that information.

Well the browser knows when it sends a cookie. So showing a [cookie] icon would be easy there. When you are in anonymous mode it does not send a cookie. (perhaps a no-cookie/cert icon - would be more precise) As for per site identity that is what the Mozilla folks were working with Aza Raskin

<http://www.azarask.in/blog/post/identity-in-the-browser-firefox/>

But until a standard is agree to there, one could already have a [cookie] icon...

For anonymous, Chrome already has an anonymous mode (though note that you don't really stay anonymous for long once you enter it, since it must still use cookies or the 'net stops working - also bookmarks are still available in anon mode).

As above the browser knows when it sends cookies: and so it can show the user that it is doing that.

I believe that Chrome experimented with per-tab personas and found that it was a terrible user experience, btw.

It does not look that bad in Aza Raskin's proposal, and the Account Manager work at Mozilla

https://wiki.mozilla.org/Labs/Weave/Identity/Account_Manager

My guess is that the project to create the multiple user work at Chrome trumped the development of good identity transparency solutions. That often happens in engineering: one good idea hides another one for a while.

In any case there is a lack of transparency in the multiple user set up that still needs to be rectified. How that is done I'll leave to UI experts. But I'll recognise a good solution whatever form it takes.

Now here with WebID we are assuming such a solution will be found by one of the browser vendors in good time, and then adopted by the others. The current interface we can agree is not good enough for sure, but the problems we are trying to solve are important enough that we can work with the current limitations of browser.

That leaves us with the importance of cross site identity. I think I have a very powerful argument in favour of its importance. It is important for a certain kind of privacy to be possible: that between two people or groups of people wishing to exchange documents that should only be visible to certain people and no others. This is the case when someone wishes to discuss something with a doctor, or when someone wishes to publish photos of people at a party without making it fully public, and in many many other circumstances. It is important for creating a distributed social network, which I will call the Social Web. The Web and the internet have always been about distribution and decentralisation of information. We want to do that using WebID in a manner that increases privacy. I will be working on showing how this can be done on the Web, and on the Web running over Tor.

Henry

Social Web Architect
<http://bblfish.net/>