Presentation

Attendees: Peter from Brave, Jason Novak and Alex Christiansen from Apple, Eric Lawrence from MS, Charlie Vazac and Nic Jansma from Akamai, Mike West, Alex Russell, Artur Janc, Yoav Weiss from Google

Yoav:
Client hints is a content negotiation mechanism that enables the browser to send specific hints to origins about the user's device, condition or preferences.
It's an opt in mechanism. The origin opts-in to receive hints, the hints can be persistent (and treated as cookies) and are only sent to first party origins.
The hints are also sent on HTTPS only, preventing passive fingerprinting on the network.
The hints are also delegatable, meaning that the first party can send the hints to specific third parties that require them.
At the same time, Client Hints is the overall mechanism and not the individual feature that use it. The features it exposes exist in JS and therefore it doesn't expose anything beyond active fingerprinting.
Fingerprinting that CH will enable will be more controllable than the JS equivalents, easily trackable and can be turned off by privacy sensitive UAs and users.
Finally, UA can be used in interesting ways to reduce fingerprinting surface that exists today.

Peter: user can see unauthorized delegation happens?
mikewest: regulators can see who is reading that
browser vendors can create gates in terms of how these hints get shared
Jason: is there a reason for this level of granularity (8 features)?
yoav: for images, you want to know DPR and dimensions and viewport width
yoav: for the others, these are used for general content negotiation
yoav: for html, serve alternate version for people with low bandwidth
alex: we will enable features based on memory, for mobile, send more features, the other way to do this is a user agent table (which isn't ideal)
concern is that with these 8, it identifies a user
mikewest: it shows the device. along with the ip address, gives you the user
mikewest: get people to use the well-lit path to share these hints, to be able to control who gets to see them, instead of people implementing their own logic
concern: nervous about privacy implications
mikewest: you can turn this off, and you can lie
Jason: you're both right, bad actors can be identified, by also putting more into the standard, the concern is that this becomes required, and people are just going to lie. if we are creating a mechanism with finger printing risk, aren't we creating systems that encourage bad behavior in the future, we will want to add another hint, which is another finger printing vector, introduces more risk
yoav: each of these features is already standard, its all already web exposed

Eric??: we should consider the fact that you can already do this in script/cookies, its worse for security and for performance, and the hints aren't introducing more risk
Jason: because some of these variables is time consuming to read, maybe that keeps attackers from using them
if we were looking at these js apis, we'd look at them now with a more critical eye
yoav: not all the js apis are supported in all user agents, and user agents can just lie for the hints that they don't want to expose
yoav: if it's worthwhile to expose to hints, it's worthwhile to expose to script
what about save data?
mikewest: opt-in is a good thing. developers can do this today, but hints makes it way easier. the use cases are clear, and it makes the end users lives better, and it makes servers be able to respond quicker
mikewest: we can argue about some of the features exposed to hints
mikewest: let's talk about the infra of hints versus should each one be implemented or not
mkiewest: there are other hints that i'd like to add that will help remove existing finger print vectors, like user agent string
mikewest: client hints allows us to... freeze user agent strings, not just portions. user agents could server browser versions as a hint. 32/64 bit. different styling options. by breaking user agent string into actual features, this infrastructure helps make the info about the machine more explicit, versus making it open to everyone, even over just http
mikewest: tls "grease" tricks the cipher suite portion of the ...
???: maybe making user agent string more structured and standard is the better way to attack this?
???: we like the mechanism, but we're worried about the details that are shared...
mikewest: client hints are not over http and not sent to third parties, so this isn't net neutral, this is net positive
yoav: not all sites will do the work to expose browsers and versions
mikewest: sites will still ask for these things, they will want to style based on os
mikewest: by giving mechanism for browsers to allow sites to give us this information, it also gives browsers the ability to use that data or not use it
Jason: i agree, but it gets tricky with ...., my problem is that it's opt-in on the document, it's not on the behalf of the user
mikewest: because the 1st party is making the request, it's possible that we could obtain user consent, hints gives researchers the ability to audit who is requesting the hints, and who they are sharing it with
Jason: we are exposing this without user mediation
mikewest: mechanism gets us above, not below status quo, these tools help us move in the right direction
Jason: should we bake in user mediation, or just leave it up to the user agent to handle that?
mikewest: i don't know how browsers can ask users to get consent
mikewest: can't have a useful web without exposing fingerprinting surfaces
mikewest: let's drive fingerprints elsewhere

Jason: why not move to the model where we say "this is a low powered device from this particular year", wouldn't that reduce the finger printing risk? and wouldn't that be enough of a hint?
yoav: that could replace device memory, this was discussed as part of the feature, schubie determined that it wasn't forward compatible
yoav: we can't get network info from that
mikewest: maybe categorizing devices helps in some places, maybe just iPhones, if google categorized some devices and good and some as bad, there would be some backlash, calling them high and low, manufactures are going to want to be in the high bucket
mikewest: some of these hints are useful, some are not useful, some are just user preferences. in iOS, user preferences are exposed. save data is like this too, preference is exposed
mikewest: in combination with ip address, you can uniquely identify
Jason: just because people can already access these things, doesn't mean that we should still expose them
mikewest: these are already exposed, and we can control it in the future if we make this first-class
mikewest: permission prompt would be hard
yoav: if you require user permission to get these hints, then sites will not use the well lit path, and then you can't control when its exposed and to home
Jason: the moving targets are the valuable hints to modify the content, like connection type, these are the hints that are only exposed in javascript
Jason: concern: you know when i'm on mobile
yoav: which is already measurable
Jason: making the finger printers have more work to do is a good thing
alex c: webkit didn't implement some of these things so as to not expose more finger printing vectors
alex c: viewport width is already finger printable
alex c: if we are worried about certain features, we could not expose those particular hints
alex c: would the spec mention that user agents can ....?
yoav: it definitely could, but might give less utility
mikewest: but cookie spec gives user agents a way to intervene...
mikewest: in spec, saying browsers can do what they want, that's reasonable
yoav: yes user agents can do that, and in spec we should note the trade off
mikewest: yes, we can determine device, but wanting to know that information is a reasonable thing for a web server to want to know, won't give you web fonts on a 3g network, this is in the end going to be better for the user
alex c: we shouldn't expose 2g/3g
Jason: if there are features we don't want to expose, we also need to lockdown the side channels, ...
yoav: we aren't going to be able to debate on all of these points, but the mechanism seems like people are ok with?
<nods>