Brit Proves Google's Eric Schmidt Totally Wrong: Super Cookies Can Track Users Even When In Incognito Mode

Thomas Fox-Brewster

January 5, 2015

It was either ignorance or disingenuousness. Or it could have just been a stupid mistake. In mid-December, Google chairman Eric Schmidt gave some unsound advice during an interview at the Cato Institute in Washington D.C, upon being quizzed about the potential for his employer to pass on information to intelligence agencies. "If you're concerned, for whatever reason, you do not wish to be tracked by federal and state authorities, my strong recommendation is to use [Google Chrome's] incognito mode, and that's what people do," he said. Many a facepalm was landed soon after his comments were transmitted to the wider world over Twitter.

Outside of the obvious flaws in Schmidt's suggestion – ISPs, websites and governments tapping the internet can still see users' traffic when Chrome's Incognito mode is on – a British researcher has now shown how "super cookies" could be used to place permanent trackers on people's PCs, tablets and smartphones. These can be created by taking advantage of an old problem, which stems back to at least 2011, and was highlighted by Sam Greenhalgh, a contractor currently doing work for retailing giant Asos, when he released a quick and simple test on Friday. In some cases, notably in Apple's Safari browser, they are apparently indestructible.

Super cookies can be created by abusing the "HTTP Strict Transport Security" (HSTS) security feature, which websites can use to tell browsers to enforce encryption, by using the HTTPS version of the site rather than the unprotected HTTP site, Greenhalgh explained. It's a tool that many support, including the Electronic Frontier Foundation (EFF), which has called for all sites to use it. Indeed, this kind of encryption can protect against snooping.

But there's a problem with HSTS. During the redirecting process from HTTP to HTTPS, a website owner could create "flags" – the super cookies – in a visitor's browser by forcing it to

store unique numbers made up of bits that would identify that user. Once that number is created, the website owner could share it with others so that users could be tracked across sites.

And these super cookies aren't disallowed or stopped during incognito browsing, even though the feature is designed to stop such tracking. The same goes for the equivalents on Apple Safari, Mozilla Firefox and Opera (Microsoft's Internet Explorer is only protected because it doesn't support HSTS at all). Some fixes have been implemented, meaning that if a user only ever visits a site over incognito and never over standard browsing, HSTS cannot be exploited to create these cookies. HSTS pins set during incognito browsing are not carried over to normal browsing.

But the problems are even more severe for Safari, the default browser on the iPhone and iPad. That's because, unlike other browsers, Safari doesn't clear HSTS flags when normal cookies – those tracking files placed on the browser during everyday browsing – are manually deleted. And they're synced with Apple's iCloud, meaning that they will be automatically downloaded even when customers' devices are wiped, said Greenhalgh, who believes this is the most concerning issue around HSTS super cookies.

Greenhalgh doesn't know of any companies who are actively exploiting this technique. "Knowing your users, understanding their browsing habits and buying patterns is a big factor in the successes of online retail. I don't think most big name online retailers would risk losing the trust of their customer base by employing nefarious tracking mechanisms like this," he told me.

Such surreptitious tracking is not unheard of, however. Verizon and AT&T were recently spotted testing out "permacookies", which inserted tracking numbers over the network when smartphone users went on the web. They weren't doing a good job of hiding their techniques either, meaning anyone could abuse them to start spying on people. There was concern the likes of the NSA would enjoy such access, given the US agency used unique cookies Google cookies to "pinpoint" targets for hacking. It wouldn't be too wild to suggest such parties would use HSTS cookies to satisfy their respective tracking initiatives.

It's possible Google has gone as far as it can in stopping HSTS tracking. By automatically deleting data related to HSTS, it may degrade security protections provided by that feature, though it may help prevent privacy abuses. "It would be likely that at the detriment to user experience that privacy enhancing browser extensions for Google Chrome and Mozilla Firefox could be developed in an effort to mitigate the observed behaviour. But, as previously noted by Google, defeating such fingerprinting is likely not practical without fundamental changes to how the web works," said Rob Cotton, chief executive officer at global information assurance specialist NCC Group.

Google declined to comment outside of the information it provided to Greenhalgh, which reiterated its developers' previous concerns about finding a balance between privacy and security.

After nearly four years of debate amongst talented coders and security pros, including the Chromium development team that builds the base code for Google's browser, it's apparent that

these kinds of super cookies might be unstoppable. Those who want guaranteed privacy will just have to trust companies won't simultaneously exploit security and erode privacy.