Engineer still concerned over Safari tracking prevention

January 24 2020, by Nancy Cohen

Credit: CC0 Public Domain

The headlines on many tech-watching sites this week amounted to one big whaaat? An anti-tracking feature in Apple's Safari browser was actually exposing private browsing habits, according to researchers outside Apple. This was all about the Intelligent Tracking Prevention (ITP) implemented by Apple's Safari browser.

The Intelligent Tracking Prevention tool became available in 2017.

Ivan Mehta in *TNW* expanded: "In 2017, Apple rolled out its ITP technology, one of the most highly regarded privacy protection kits for the web around the world. The system clears out first-party cookies regularly and blocks third-party cookies by default, making it difficult for advertisers to track users."

The head-scratching grew more intense. The researcher team from Google told Apple about the problem with some flaws back in August 2019 and in December an Apple blog post said browser issues were addressed.

An Apple engineer said in the blog WebKit in December that the matter had been addressed—the news was encouraging to any user worried about tracking fallouts. Apple had produced a fix and said thank you to Google.

But researchers at Google raised issues still.

Financial Times had a much quoted story, and other news gatherers also talked about, a published paper by Google researchers that found problems, and the paper was published on Jan. 21. "Information Leaks via Safari's Intelligent Tracking Prevention" is the title of the Google report; the authors were Artur Janc, Krzysztof Kotowicz, Lukas Weichselbaum and Roberto Clapis. Their focus still is the tool that Apple offered to counter web tracking.

Actually, according to the Google team's report on this, the Information

Security Engineering team at Google first learned about the flaws just during "a routine security review." That is when they found security and privacy issues in Safari's Intelligent Tracking Prevention design.

In the Google report, they wrote: "The authors of this report believe strongly in improving the privacy posture of the web and applaud Safari developers' ongoing efforts in this area. At the same time we would like to note that all changes to the web platform that affect its fundamental security properties (such as modifying the behavior of cross-site resource fetches) carry the risk of compromising user privacy and/or security unless special care is taken to understand their impact on the platform. We look forward to collaborating with Apple on future security and privacy improvements to the web."

End of story? After all, Reuters has reported on Jan. 22 that "An Apple spokesman on Wednesday confirmed that the flaws found by Google and highlighted in the Financial Times' story were patched last year."

On the Dec. 10 post, John Wilander had said, "We have devised three ITP enhancements that not only fight detection of differing treatment but also improve tracking prevention in general."

Cookies was one of the issues addressed. Wilander said, "ITP will now block all third-party requests from seeing their cookies, regardless of the classification status of the third-party domain, unless the first-party website has already received user interaction."

Another of the enhancements was downgrading referrer headers.

"ITP now downgrades all cross-site request referrer headers to just the page's origin. Previously, this was only done for cross-site requests to classified domains.

Wilander gave readers an example. A request to images.example that would previously contain the referrer header "store.example/baby/strollers/d … oller-navy-blue.html" will now be reduced to just "store.example/".

The Wilander blog post in December had posted equally nice things to say about Google. "Thanks To Google" was the header of a paragraph in the WebKit blog post.

"We'd like to thank Google for sending us a report in which they explore both the ability to detect when web content is treated differently by tracking prevention and the bad things that are possible with such detection. Their responsible disclosure practice allowed us to design and test the changes detailed above. Full credit will be given in upcoming security release notes."

So, can we all go home now? Wait a minute. Alfred Ng reporting for CNET talked about a tweet from Google Chrome engineering director Justin Schuh that Apple has not fixed certain Safari tracking prevention problems.

Schuh had tweeted: "It has not. I explained elsewhere that Apple's blog post was confusing to the team that provided the report. The post was made during a disclosure extension Apple had requested, but didn't disclose the vulnerabilities, and the changes mentioned didn't fix the reported issues."

Rami Tabari, *Laptop Mag*, said, "a number of the issues discussed in this paper were addressed in Safari 13.0.4 and iOS 13.3, which released in December 2019." Yet *Laptop Mag*'s subhead: "Apple fixed it, but there's still a threat."

At the time of this writing, Silicon.co.uk reported that Apple fixed

Safari's tracking flaws but the Google engineer disagreed. Tom Jowitt explained that it seemed as though the Google engineer did not think that Apple actually patched the problem.

Also, at the time of this writing, Bloomberg had this to say: "Wednesday's paper concluded that the problems go beyond the issues that Apple addressed. Instead of making a big list of cookies to block, Apple's ITP continuously learns what websites users visit and which kinds of cookies try to hitch a ride. Over time, this creates unique cookie-blocking algorithms for each web surfer that can be used to identify and track them, according to the paper."

The report from Gerrit De Vynck, Bloomberg Technology, while not giving a hard answer, was especially insightful. It took its readers into the larger domain of Apple-Google browser marketplace dynamics.

Google's Chrome and Apple's Safari are two of the most popular web browsers, with Chrome used by more people but with Safari's domination on iPhones, he wrote. "Apple has been touting Safari privacy features to persuade more consumers to use it. Apple first introduced Intelligent Tracking Prevention in 2017."

De Vynck was aware how "Privacy advocates have lauded Apple's approach to tracking, and criticized Google for taking so long to do the same. But the paper suggests Apple may have to go back to the drawing board to find a new way to block tracking."

More information: Information Leaks via Safari's Intelligent Tracking Prevention, arXiv:2001.07421 [cs.CR] arxiv.org/abs/2001.07421

Citation: Engineer still concerned over Safari tracking prevention (2020, January 24) retrieved 4 May 2024 from https://techxplore.com/news/2020-01-safari-tracking.html