New web tracking technique is bypassing privacy protections

December 14 2022, by Ioana Patringenaru

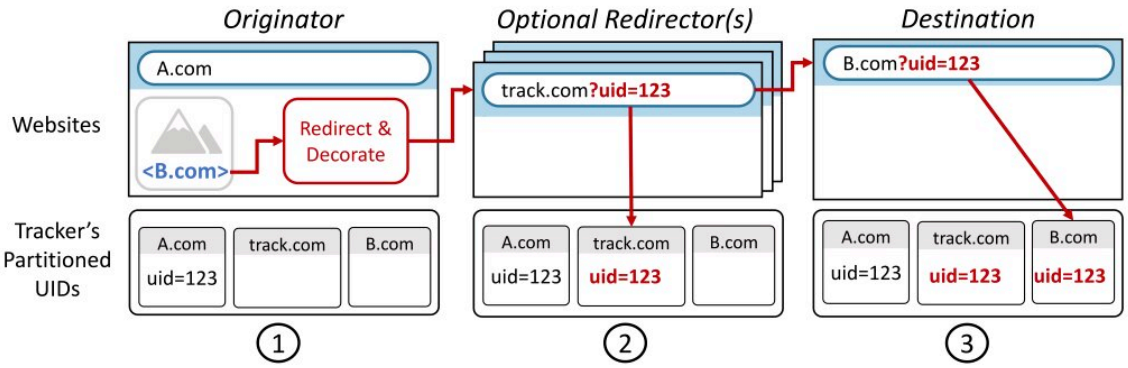

Figure 2: How UID smuggling allows trackers to circumvent partitioned storage.

This chart shows how advertisers can deploy user ID smuggling to track users on the web. Credit: University of California San Diego

Advertisers and web trackers have been able to aggregate users' information across all of the websites they visit for decades, primarily by placing third-party cookies in users' browsers.

Two years ago, several browsers that prioritize user privacy—including Safari, Firefox, and Brave—began to block third-party cookies for all users by default. This presents a significant issue for businesses that place ads on the web on behalf of other companies and rely on cookies to track click-through rates to determine how much they need to get

paid.

Advertisers have responded by pioneering a new method for tracking users across the Web, known as user ID (or UID) smuggling, which does not require third-party cookies. But no one knew exactly how often this method was used to track people on the Internet.

Researchers at UC San Diego have for the first time sought to quantify the frequency of UID smuggling in the wild, by developing a measurement tool called CrumbCruncher. CrumbCruncher navigates the Web like an ordinary user, but along the way, it keeps track of how many times it has been tracked using UID smuggling.

The researchers found that UID smuggling was present in about 8 percent of the navigations that CrumbCruncher made. They presented these results at the Internet Measurement Conference Oct. 25 to 27, 2022 in Nice, France. The team is also releasing both their complete dataset and their measurement pipeline for use by browser developers.

The team's main goal is to raise awareness of the issue with browser developers, said first author Audrey Randall, a computer science Ph.D. student at UC San Diego. "UID smuggling is more widely used than we anticipated," she said. "But we don't know how much of it is a threat to user privacy."

UID smuggling can have legitimate uses, the researchers say. For example, embedding user IDs in URLs can allow a website to realize a user is already logged in, which means they can skip the login page and navigate directly to content. It's also a tool that a company that owns websites with different domains can use to track user traffic.

It's also, of course, a tool for affiliate advertisers to track traffic and get paid. For example, a blogger who advertises a product using affiliate

links might be paid a commission if anyone clicks their links and then makes a purchase. UID smuggling can identify which blogger should get the commision.

But there are potentially more dangerous uses that researchers worry about. For example, a data broker could use UID smuggling to gather a database of users' Internet navigation.

Researchers also did a small exercise where they manually blocked UID smuggling for several navigations. They found that this had a minimal impact on website functionality. Next steps could include building a tool to block UIDs. But researchers warn that this likely will only be another step in an ongoing cat-and-mouse game.

"Whatever we do, the game won't end unless we can find a solution that allows the ad industry to remain profitable while still preserving user privacy," said first author Randall.

More information: Paper (PDF): Measuring UID Smuggling in the Wild

Provided by University of California - San Diego