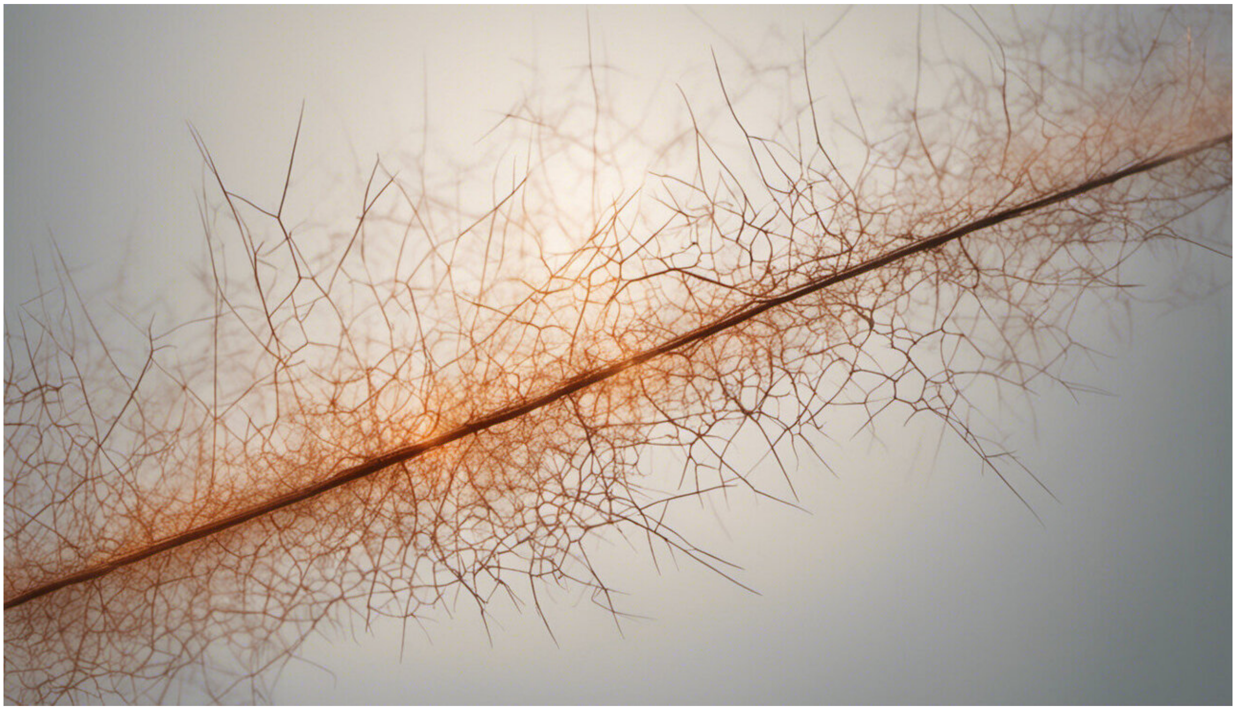
TechXplore

Novel technique tracks more web users across browsers

February 13 2017, by Kurt Pfitzer



Credit: AI-generated image (disclaimer)

For good or ill, what users do on the web is tracked. Banks track users as an authentication technique, to offer their customers enhanced security protection. Retailers track customers and potential customers in order to deliver personalized service tailored to their tastes and needs.

The method commonly used for tracking is called web fingerprinting. Web fingerprinting is a way of collecting information that can be used to fully or partially identify a given user, even when cookies are disabled.

Such techniques have been evolving quickly. Yet, the most advanced and commonly used methods track users in a single browser only.

Now a team of researchers led by Yinzhi Cao, assistant professor computer science and engineering—and including graduate student Song Li of Lehigh and Erik Wijmans of Washington University in St. Louis—has developed the first cross-browser fingerprinting technique to use machine-level features to identify users.

The researchers describe the technique in a paper titled "(Cross-) Browser Fingerprinting via OS and Hardware Level Features." Cao and his colleagues are scheduled to present their findings at the Internet Society's Network and Distributed System Security (NDSS) Symposium from February 26 through March 1 in San Diego, Calif.

In their paper, the authors claim to be the first group "to use many novel OS [operating system] and hardware features, especially computer graphics ones, in both single- and cross-browser fingerprinting. Particularly, our approach with new features can successfully fingerprint 99.24 percent of users as opposed to 90.84 percent for AmIUnique, i.e., state of the art, on the same dataset for single-browser fingerprinting."

In addition, the authors say their technique can achieve higher uniqueness rates than the only cross-browser approach in the literature with similar stability.

"The only other cross-browser fingerprinting work uses the IP [Internet Protocol] address as the main feature by which to identify users," says Cao. "This method has been criticized as too unstable as people use the internet at home, work and on different devices. Using an IP address is too dynamic and unreliable."

The novel approach developed by Cao's group adopts OS and hardware levels features including graphic cards exposed by WebGL, audio stack by Audio-Context, and CPU (central processing unit) by hardwareConcurrency. In addition to being able to uniquely identify more users than AmIUnique for single-browser fingerprinting, and the only other cross-browser fingerprinting technique in the literature, the group's approach is highly reliable. According to their study, the removal of any single feature decreases the accuracy by at most only 0.3 percent.

The group used crowdsourcing for data collection, asking participants to visit their website using two different browsers of their choice and encouraging them to use a third browser by offering additional payment.

Cao says the ideal next step for this work would be for a financial institution to adopt the approach as a way to provide multi-factor authentication for their customers.

"Our goal is for people to use it," he says.

Provided by Lehigh University

Citation: Novel technique tracks more web users across browsers (2017, February 13) retrieved 18 April 2024 from
https://techxplore.com/news/2017-02-technique-tracks-web-users-browsers.html