Share button may share your browsing history, too

July 22 2014

Cwm fjordbank glyphs vext quiz
Cwm fjordbank glyphs vext (

An exact replica of the image rendered by a real-world canvas fingerprinting script. The script uses a so-called ‘perfect pangram’, “Cwm fjordbank glyphs vext quiz”, which contains all the letters of the English alphabet. This maximizes the diversity of the image outcomes with the shortest possible string.

One in 18 of the world's top 100,000 websites track users without their consent using a previously undetected cookie-like tracking mechanism embedded in 'share' buttons. A new study by researchers at KU Leuven and Princeton University provides the first large-scale investigation of the mechanism and is the first to confirm its use on actual websites.

The mechanism, called "canvas fingerprinting", uses special scripts – the coded instructions that tell your browser how to render a website – to exploit the browser's so-called 'canvas', a browser functionality that can be used to draw images and render text.

When a user visits a website encoded with canvas fingerprinting software, a first script tells the user's browser to print an invisible string of text on the browser's canvas. Another script then instructs the browser to read back data about the pixels in the (invisibly) rendered image.

These data contain important information about the user's browser type, graphics card, system fonts and even display properties. Because this grouping of data is highly likely to be unique for each user, it can be reliably associated to individual users, like a fingerprint.

Cookies

Once a website has determined a device's fingerprint, it can easily recognize the user on subsequent site visits, much in the same way cookies do.

But while unwanted cookies can be flagged or blocked to enhance a user's online privacy, there is no available solution for doing so with fingerprints.

In this study, the researchers used automated 'crawlers' to scan the world's top 100,000 websites for canvas fingerprinting scripts. They found canvas fingerprinting scripts on 5,542 of the internet's top 100,000 websites, a prevalence of 5.5 percent.

Previous studies on related browser fingerprinting techniques reported a prevalence of 0.4 percent and 1.5%, respectively, although they are not directly comparable to the current study since they measured different types of fingerprinting techniques.

While researchers demonstrated the feasibility of canvas fingerprinting as a tracking mechanism in 2012, this is the first time it has been observed on real websites and traced back to specific provider domains. Analyses of the real-world scripts reveal that fingerprinters are going beyond the techniques known by the academic research community.

AddThis

Surprisingly, the researchers traced 95 percent of canvas fingerprinting scripts back to a single company: AddThis. AddThis is the world's largest content sharing platform and provides free website plugins such as share buttons, follow buttons and content recommendation features. The company reaches an estimated 97.2% of Internet users in the United States and receives 103 billion page views each month.

Can users protect themselves against canvas fingerprinting? Acar and his colleagues studied the effect of ad-industry opt-out tools offered by the Network Advertising Initiative (NAI) and the European Interactive Digital Advertising Alliance. No websites included in the opt-lists stopped collecting canvas fingerprints after activating the opt-out option.

At present, only one browser, Tor, can prevent canvas fingerprinting scripts, but this added security comes with major trade-offs in performance, functionality and content availability.

Many websites, including sensitive sites such as health and government websites, unknowingly contain canvas fingerprinting – by using one of AddThis' free plug-ins for example.

The researchers are concerned by the growing prevalence of canvas fingerprinting , says Gunes Acar, the first author of the study: "This is an advanced tracking mechanism that misuses browser features to enable the circumvention of users' tracking preferences. We hope that our results will lead to better defenses, increase accountability for companies deploying sticky tracking techniques and an invigorated and informed public and regulatory debate on increasingly resilient tracking techniques."

More information: securehomes.esat.kuleuven.be/~ … ersistent/index.html

Provided by KU Leuven

Citation: Share button may share your browsing history, too (2014, July 22) retrieved 17 May 2024 from https://phys.org/news/2014-07-button-browsing-history.html