PHYS.ORG

How websites watch your every move and ignore privacy settings

November 27 2017, by Yijun Yu

Credit: Karolina Grabowska from Pexels

Hundreds of the world's top websites routinely track a user's every keystroke, mouse movement and input into a web form – even before it's submitted or later abandoned, according to the results of a study from researchers at Princeton University.

And there's a nasty side-effect: personal identifiable data, such as medical information, passwords and credit card details, could be revealed when users surf the web – without them knowing that companies are monitoring their browsing behaviour. It's a situation that should alarm anyone who cares about their privacy.

The Princeton researchers found it was difficult to redact personally identifiable information from browsing behaviour records – even, in some instances, when users have switched on privacy settings such as Do Not Track.

The research found that third party tracking services are used by hundreds of businesses to monitor how users navigate their websites. This is proving to be increasingly challenging as more and more companies beef-up security and shift their sites over to encrypted HTTPS pages.

To work around this, session-replay scripts are deployed to monitor user interface behaviour on websites as a sequence of time-stamped events, such as keyboard and mouse movements. Each of these events record additional parameters – indicating the keystrokes (for keyboard events) and screen coordinates (for mouse movement events) – at the time of interaction. When associated with the content of a website and web address, this recorded sequence of events can be exactly replayed by another browser that triggers the functions defined by the website.

What this means is that a third person is able to see, for example, a user entering a password into an online form – which is a clear privacy breach. Websites that employ third party analytics firms to record and replay such behaviour is, they argue, in the name of "enhancing user experience". The more they know what their users are after, the easier it is to provide them with targeted information.

While it's not news that companies are monitoring our behaviour as we surf the web, the fact that scripts are quietly being deployed to record individual browser sessions in this way has concerned the study's co-author, Steven Englehardt, who is a PhD candidate at Princeton.

"Collection of page content by third-party replay scripts may cause sensitive information, such as medical conditions, credit card details, and other personal information displayed on a page, to leak to the third-party as part of the recording," he wrote. "This may expose users to identity theft, online scams and other unwanted behaviour. The same is true for the collection of user inputs during checkout and registration processes."

Websites logging keystrokes has been an issue known for a while to cybersecurity experts. And Princeton's empirical study raises valid concerns about users having little or no control over their surfing behaviour being recorded in this way.

So it's important to help users control how their information is shared online. But there are increasing signs of usability trumping security measures that are designed to keep our data safe online.

Usability vs security

Password managers are used by millions of people to help them easily keep a record of different passwords for different sites. The user of such a service only needs to memorise one key password.

Recently, a group of researchers at the University of Derby and the Open University discovered that the offline clients of password manager services were at risk of exposing the main key password when stored as plain text in memory that could be sniffed or dumped by whole system attacks.

User experience is not an excuse for tolerating security flaws.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How websites watch your every move and ignore privacy settings (2017, November 27) retrieved 17 July 2024 from https://phys.org/news/2017-11-websites-privacy.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.