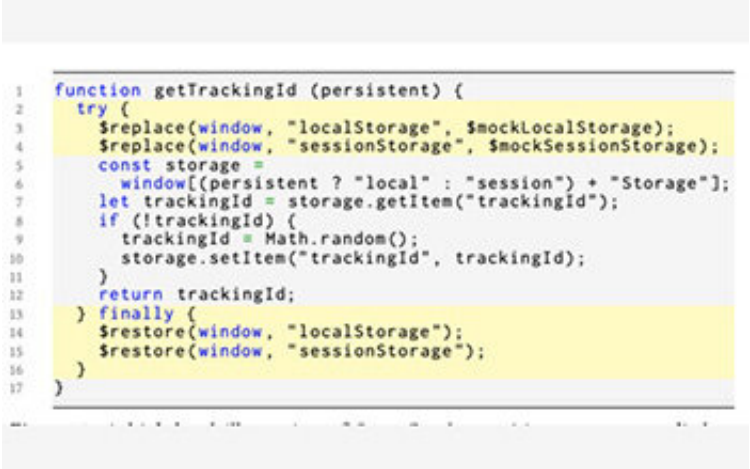
New tool protects users' private data while they browse

December 14 2021



SugarCoat modifies code to protect private data. Credit: UCSD

Computer scientists funded by the U.S. National Science Foundation and affiliated with the University of California San Diego and Brave Software have developed a tool that will increase protections for users' private data while they browse the web.

The tool, named SugarCoat, targets scripts that harm users' privacy—for example, by tracking their browsing history around the web—yet are essential for the websites that embed them to function. SugarCoat replaces these scripts with others that have the same properties, minus the privacy-harming features. SugarCoat is designed to be integrated into existing privacy-focused browsers like Brave, Firefox and Tor as well as

browser extensions like uBlock Origin. SugarCoat is open source and is currently being integrated into the Brave browser.

"SugarCoat is a practical system designed to address the lose-lose dilemma that privacy-focused tools face today: Block privacy-harming scripts but break websites that rely on them, or keep sites working, but give up on privacy," said Deian Stefan of UC San Diego. "SugarCoat eliminates this trade-off by allowing the scripts to run, thus preserving compatibility, while preventing the scripts from accessing user-private data."

The researchers described their work at the ACM Conference on Computer and Communications Security.

"SugarCoat integrates with existing content-blocking tools, like ad blockers, to empower users to browse the Web without giving up their privacy," said Michael Smith, who is leading the project.

Most existing content-blocking tools make very coarse-grained decisions. They either totally block or totally allow a script to run, based on whether it appears on a public list of privacy-harming scripts. In practice, though, some scripts are both privacy-harming and necessary for websites to function, and most tools inevitably choose to make an exception and allow these scripts to run. Today, there are more than 6,000 exception rules letting through these privacy-harming scripts.

Instead of blocking a script entirely or allowing it to run, content-blocking tools can replace source code with an alternative privacy -preserving version. For example, instead of loading popular website analytics scripts which also track users, content-blocking tools replace these scripts with fake versions that look the same. This ensures that the content-blocking tools are not breaking web pages that embed these scripts and that the scripts cannot access private data—and thus report it

back to analytics companies.

More information: Michael Smith et al, SugarCoat: Programmatically Generating Privacy-Preserving, Web-Compatible Resource Replacements for Content Blocking, *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (2021). DOI: 10.1145/3460120.3484578

Provided by National Science Foundation