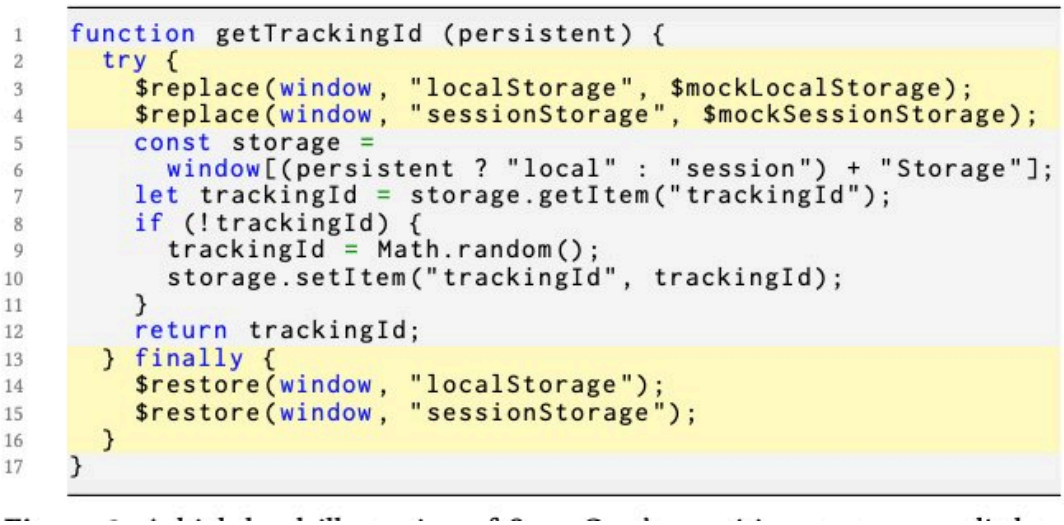
This tool protects your private data while you browse

November 18 2021



```
function getTrackingId (persistent) {
  try {
    $replace(window, "localStorage", $mockLocalStorage);
    $replace(window, "sessionStorage", $mockSessionStorage);
    const storage =
      window[(persistent ? "local" : "session") + "Storage"];
    let trackingId = storage.getItem("trackingId");
    if (!trackingId) {
      trackingId = Math.random();
      storage.setItem("trackingId", trackingId);
    }
    return trackingId;
  } finally {
    $restore(window, "localStorage");
    $restore(window, "sessionStorage");
  }
}
```

A high-level illustration of how SugarCoat modified code within API to protect private data. Credit: University of California San Diego

A team of computer scientists at 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 scripts 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, and 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, an assistant professor in the UC San Diego Department of Computer Science and Engineering. "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 will describe their work at the ACM Conference on Computer and Communications Security (CCS) taking place in Seoul, Korea, Nov. 14 to 19, 2021.

"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, a Ph.D. student in Stefan's research group, 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.

There is a better approach, though. Instead of blocking a script entirely

or allowing it to run, content-blocking tools can replace its 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 can't access private data (and thus report it back to the analytics companies). To date, crafting such privacy-preserving replacement scripts has been a slow, manual task even for privacy engineering experts. uBlock Origin, for example, maintains replacements for only 27 scripts, compared to the over 6,000 exception rules.

How SugarCoat changes the game

The researchers developed SugarCoat precisely to address this gap by automatically generating privacy-preserving replacement scripts. The tool uses the PageGraph tracing framework—Smith was key to the development of the framework—to follow the behavior of privacy-harming scripts throughout the browser engine.

SugarCoat scans this data to identify when and how the scripts talk to Web Platform APIs that expose privacy-sensitive data. SugarCoat then rewrites the scripts' source code to talk to fake "SugarCoated" APIs instead, which look like the Web Platform APIs but don't actually expose any private data.

To evaluate the impact of SugarCoat on Web functionality and performance, the team integrated the rewritten scripts into the Brave browser; they found that SugarCoat effectively protected users' private data without impacting functionality or page load performance. SugarCoat is now being deployed in production at Brave.

"Brave is excited to start deploying the results of the year-long

SugarCoat research project," said Peter Snyder, senior privacy researcher and director of privacy at Brave Software. "SugarCoat gives Brave and other privacy projects a powerful, new capability for defeating online trackers, and helps keep users in control of the Web."

More information: Michael Smith et al, SugarCoat: Programmatically Generating Privacy-Preserving, Web-Compatible Resource Replacements for Content Blocking is available as a PDF at brave.com/wp-content/uploads/2 … garcoat-ccs-2021.pdf

Provided by University of California - San Diego