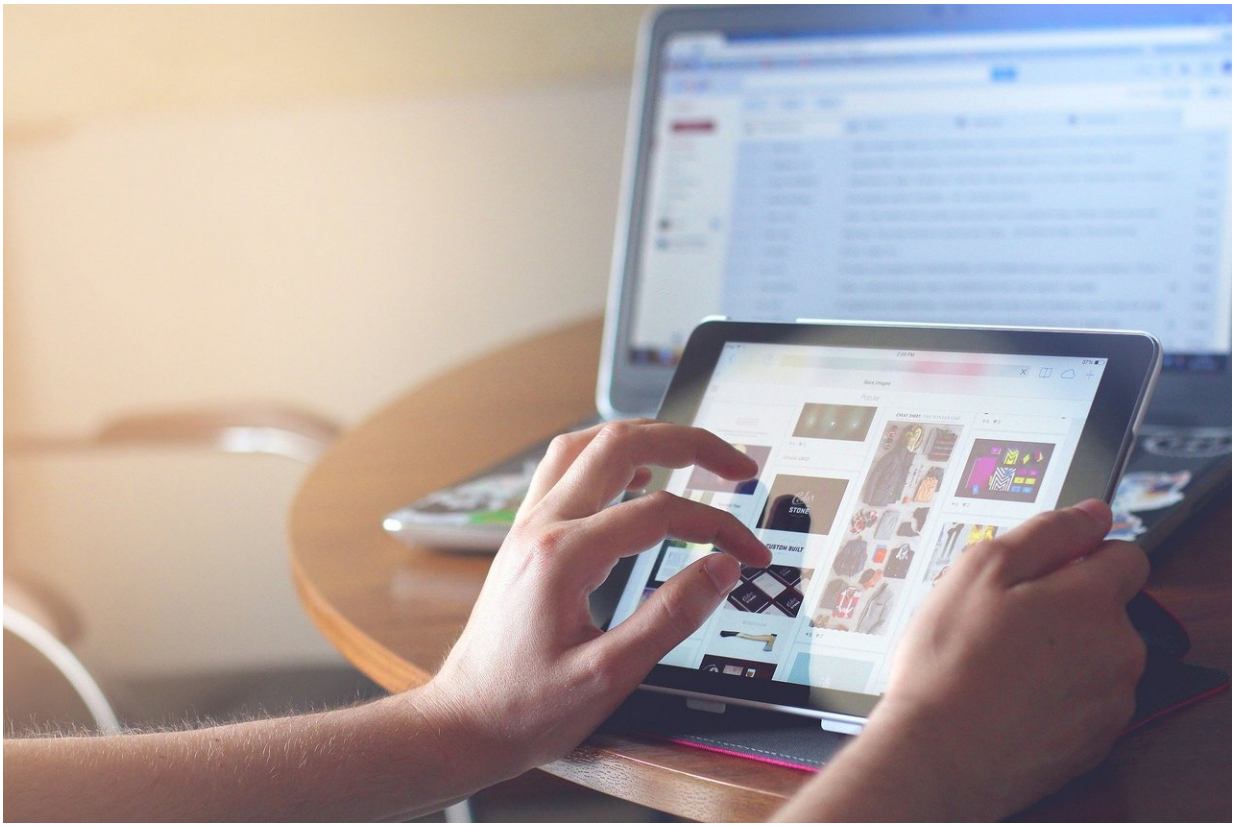
Bloated browser functionality presents unnecessary security, privacy risks

October 24 2017



Credit: CC0 Public Domain

Modern website browsers provide an incredibly broad range of features, with more and more capabilities being added every day.

New research by computer scientists at the University of Illinois at Chicago have identified numerous browser functionalities rarely used or needed by websites, but which pose substantial security and privacy risks to web surfers. Blocking website access to unnecessary browser functionality would help reduce these risks.woman using laptop

Peter Snyder, a graduate student of computer science at UIC, and his colleagues looked at the costs and benefits associated with websites having access to 74 different types of functionality (collectively called web application programming interface, or API). They measured how frequently each of these features was used on websites, and how likely each was to pose a risk to security or privacy. Features with a low benefit to users, but a high security risk, were flagged as those that could be blocked to improve security, Snyder explained.

"For example, browsers allow websites to perform low-level graphics calculations," said Snyder. "We found that this functionality is rarely used on honest websites, but that malicious sites can use it to harm users' privacy and security." Allowing all websites to access this feature is "a bad cost-benefit trade-off," Snyder explained.

Other examples of high-risk, low-benefit functionality the researchers uncovered included code that lets browsers detect light levels in a room, perform fine-grained timing operations and perform advanced audio synthesis operations.

Snyder and his colleagues will present their findings at the Association for Computing Machinery Conference on Computer and Communications Security in Dallas on October 31.

In their analysis, the researchers used Firefox as their test browser, since it is the most popular, fully open-source browser. Findings from the Firefox browser should generalize to other browsers, Snyder explained,

because it has access to an almost identical suite of capabilities as other common browsers like Chrome and Internet Explorer.

"Ultimately we saw that about 25 percent of web API posed high risks to security and privacy and could be blocked without breaking websites," Snyder said. He explained that by blocking risky functionality, the amount of code a website accesses is also reduced. "The less code you have available through the web API, the safer websites you'll have."

Based on their findings, Snyder's team developed a browser extension that allows users to selectively block browser functionality to improve safety when it comes to surfing the web.

Brave, a company focused on providing safer web browsing and founded by the inventor of JavaScript and the co-founder of Mozilla, plans on incorporating parts of the research into its open-source web browser, Brave Browser.

Provided by University of Illinois at Chicago