Issued 11/2/18

New Techniques Expose your Browsing History to Attackers

Security researchers at UC San Diego and Stanford have discovered four new ways to expose Internet users' browsing histories. These techniques could be used by hackers to learn which websites users have visited as they surf the web. The techniques fall into the category of "history sniffing" attacks, a concept dating back to the early 2000s. But the attacks demonstrated by the researchers at the 2018 USENIX Workshop on Offensive Technologies (WOOT) in Baltimore can profile or 'fingerprint' a user's online activity in a matter of seconds, and work across recent versions of major web browsers. All of the attacks the researchers developed in their WOOT 2018 paper worked on Google Chrome. Two of the attacks also worked on a range of other browsers, from Mozilla Firefox to Microsoft Edge, as well various security-focused research browsers. The only browser which proved immune to all of the attacks is the Tor Browser, which doesn't keep a record of browsing history in the first place. After conducting an effective history sniffing attack, a criminal could carry out a smart phishing scheme, which automatically matches each victim to a faked page corresponding to their actual bank. The phisher preloads the attack code with their list of target banking websites, and conceals it in, for example, an ordinary-looking advertisement. When a victim navigates to a page containing the attack, the code runs through this list, testing or 'sniffing' the victim's browser for signs that it's been used to visit each target site. When one of these sites tests positive, the phisher could then redirect their victim to the corresponding faked version. History sniffing can also be deployed by legitimate, yet unscrupulous, companies, for purposes like marketing and advertising. A 2010 study from UC San Diego documented widespread commercial abuse of previously known history sniffing

attack techniques, before these were subsequently fixed by browser vendors. The researchers' four attacks target flaws in relatively new browser features. For example, one attack takes advantage of a feature added to Chrome in 2017, dubbed the "CSS Paint API", which lets web pages provide custom code for drawing parts of their visual appearance. Using this feature, the attack measures when Chrome re-renders a picture linked to a particular target website URL, in a way invisible to the user. When a re-render is detected, it indicates that the user has previously visited the target URL. "This attack would let an attacker check around 6,000 URLs a second and develop a profile of a user's browsing habits at an alarming rate," said Fraser Brown, a Ph.D. student at Stanford, who worked closely with Smith. Though Google immediately patched this flaw–the most egregious of the attacks that the researchers developed–the computer scientists describe three other attacks in their WOOT 2018 paper that, put together, work not only on Chrome but Firefox, Edge, Internet Explorer, but on Brave as well. The Tor Browser is the only browser known to be totally immune to all the attacks, as it intentionally avoids storing any information about a user's browsing history.