Several top websites use device fingerprinting to secretly track users

A new study by KU Leuven-iMinds researchers has uncovered that 145 of the Internet's 10,000 top websites track users without their knowledge or consent. The websites use hidden scripts to extract a device fingerprint from users' browsers. Device fingerprinting circumvents legal restrictions imposed on the use of cookies and ignores the Do Not Track HTTP header. The findings suggest that secret tracking is more widespread than previously thought.

Device fingerprinting, also known as browser fingerprinting, is the practice of collecting properties of PCs, smartphones and tablets to identify and track users. These properties include the screen size, the versions of installed software and plugins, and the list of installed fonts. A 2010 study by the Electronic Frontier Foundation (EFF) showed that, for the vast majority of browsers, the combination of these properties is unique, and thus functions as a 'fingerprint' that can be used to track users without relying on cookies. Device fingerprinting targets either Flash, the ubiquitous browser plugin for playing animations, videos and sound files, or JavaScript, a common programming language for web applications.

This is the first comprehensive effort to measure the prevalence of device fingerprinting on the Internet. The team of KU Leuven-iMinds researchers analysed the Internet's top 10,000 websites and discovered that 145 of them (almost 1.5%) use Flash-based fingerprinting. Some Flash objects included questionable techniques such as revealing a user's original IP address when visiting a website through a third party (a so-called proxy).

The study also found that 404 of the top 1 million sites use JavaScript-based fingerprinting, which allows sites to track non-Flash mobile phones and devices. The fingerprinting scripts were found to be probing a long list of fonts – sometimes up to 500 – by measuring the width and the height of secretly-printed strings on the page.

The researchers identified a total of 16 new providers of device fingerprinting, only one of which had been identified in prior research. In another surprising finding, the researchers found that users are tracked by these device fingerprinting technologies even if they explicitly request not to be tracked by enabling the Do Not Track (DNT) HTTP header.

The researchers also evaluated *Tor Browser* and *Firegloves*, two privacy-enhancing tools offering fingerprinting resistance. New vulnerabilities – some of which give access to users' identity – were identified.

Device fingerprinting can be used for various security-related tasks, including fraud detection, protection against account hijacking and anti-bot and anti-scraping services. But it is also being used for analytics and marketing purposes via fingerprinting scripts hidden in advertising banners and web widgets.

To detect websites using device fingerprinting technologies, the researchers developed a tool called FPDetective. The tool crawls and analyses websites for suspicious scripts. This tool will be freely available at http://homes.esat.kuleuven.be/~gacar/fpdetective/ for other researchers to use and build upon.

The findings will be presented at the 20th ACM Conference on Computer and Communications

Security this November in Berlin.

Contact
Gunes Acar (ESAT/COSIC)
gunes.acar@esat.kuleuven.be
+32 487 125 633