Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints

https://hal.inria.fr/hal-01285470v2/document

Worldwide, the number of people and the time spent browsing the web keeps increasing. Accordingly, the technologies to enrich the user experience are evolving at an amazing pace. Many of these evolutions provide for a more interactive web (e.g., boom of JavaScript libraries, weekly innovations in HTML5), a more available web (e.g., explosion of mobile devices), a more secure web (e.g., Flash is disappearing, NPAPI plugins are being deprecated), and a more private web (e.g., increased legislation against cookies, huge success of extensions such as Ghostery and AdBlock). Nevertheless, modern browser technologies, which provide the beauty and power of the web, also provide a darker side, a rich ecosystem of exploitable data that can be used to build unique browser fingerprints. Our work explores the validity of browser fingerprinting in today's environment. Over the past year, we have collected 118,934 fingerprints composed of 17 attributes gathered thanks to the most recent web technologies. We show that innovations in HTML5 provide access to highly discriminating attributes, notably with the use of the Canvas API which relies on multiple layers of the user's system. In addition, we show that browser fingerprinting is as effective on mobile devices as it is on desktops and laptops, albeit for radically different reasons due to their more constrained hardware and software environments. We also evaluate how browser fingerprinting could stop being a threat to user privacy if some technological evolutions continue (e.g., disappearance of plugins) or are embraced by browser vendors (e.g., standard HTTP headers). ==