How Unique Is Your Web Browser?

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

The paper points out browser fingerprinting problem and investigates the real world effectiveness of browser fingerprinting algorithms. They defined a fingerprinting algorithm and collected fingerprints (commonly or less commonly used characteristics that browsers provide to websites) from 470,161 browsers, which are used to visit the website "https://panopticlick.eff.org", by the participants. These browser statistics are collected by making static http requests or collected from AJAX and then the measurements are grouped together into 8 different strings. They observed that "the distribution of fingerprint contains at least 18.1 bits of entropy, meaning that if one browser is picked at random, at best we expect that only one in 286,777 other browsers will share its fingerprint. They also claim that, among the browsers containing flash or java, the situation is worse (average browser having at least 18.8 bits of identifying characteristics). The authors also show that, even if the fingerprints changed rapidly (they change over time in browsers), simple heuristics can detect the previously observed fingerprint of the browser with "over 99% of correct guesses and over 0.8% of false positive rate"[1]. Paper also discusses the countermeasures to protect against the fingerprinting threat. They claim that, "There is a trade-off between protection against fingerprint-ability and certain kinds of debuggability, which in current browsers is weighted heavily against privacy."[1]

2 Contribution

Paper investigates, the degree to which the web browsers are subjected to "device fingerprinting"[1] problem. With their results they show the severity of the threat. They observed stability of fingerprints in the browser and the factors affecting (or contributing) that. They also give the countermeasures against the 'device fingerprinting' problem.

3 Strengths

I liked the fingerprint change detection algorithm given by the authors, it is really simple to understand. I also liked the different types of graphs provided by the authors, which help in understanding and getting to know the results visually (specifically I liked the graph given related to the Surprisal distributions for different categories of browser). I also liked that they pointed out the issues with programs provided by the companies like adobe.

4 Limitations

As suggested by the authors, tor project may be the good option, but it has several drawbacks (such as password sniffing at exit code, etc.) and performance implications.

5 Future Work

The authors mentioned that Mozilla actually exposes two different plugin orderings based on different inode timestamps, but could not test this claim. This maybe included in the future work. Also, as authors claimed, their algorithm can be further improved by adding measurements.

References

[1] Peter Eckersley *How Unique Is Your Web Browser?*