Lane Gramling
EECS 700
Reading 16

Summary - Panopticlick: How unique is your browser?

This paper focuses on the technique of using information available through HTTP requests and other ubiquitous browsing features to uniquely identify browsers through device fingerprinting. The information they record ranges from a number of seemingly innocent pieces of information like browser version and system fonts, to more immediately apparent tracking information such as HTTP cookies, flash cookies, and other device information. They undertook a large (albeit biased, although arguably *against* their goal) case study and claimed to achieve a guess accuracy rate of 99.1% of study participants measured as reasonably identifiable.

Contributions

Before diving into its novel contributions, the paper first explains the angle of approach taken with its techniques, enumerating an alarmingly large list of pieces of information that can be used in browser fingerprinting. These pieces of information, as stated before, range anywhere from tracking more immediately obvious HTTP cookies and flash cookies, to observing more obscure things such as system fonts, CPU clock skew, and millisecond-order time delays in a client's communication with a server.

Viewing the forest from above, the paper makes its first major contribution by exploring the mathematical foundations describing the effectiveness of their browser fingerprinting techniques, done so through deriving a set of equations used to quantify a few key metrics. Examples of these include the 'surprisal' of a given browser, described as the binary logarithm of the discrete probability function of *n* useful browser traits; the entropy of the surprisal distribution, supplying the expected average value of a given browser's surprisal metric; lastly, an equation describing these two metrics in terms of a given fingerprint, modifying the original discrete probability distribution function to be expressed as a conditional in relationship to other data points upon which it is linearly dependent.

The next major contribution of the paper is an outline of their strategy in data collection and the results subsequently obtained. By development of interest through media outlets, a large sample size was amassed and the aforementioned information was collected, where the aforementioned algorithms were then used to compute the uniqueness of each browser who participated in their test.

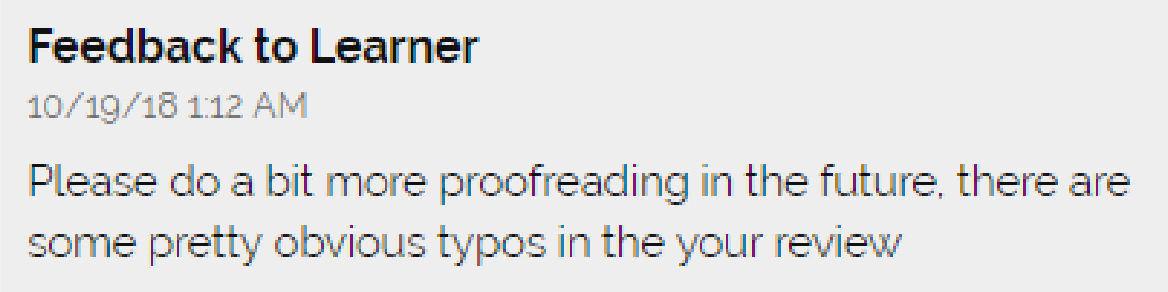
The results described by the author indicate a very high success rate in unique identification, even capable of detecting a browser retesting after a change in IP address in the case that the browser accepted cookies. Further breaking down the results, the author notes that 83.6% were identified as unique in the sample, with 8.1% exhibiting an anonymity set of size 10 and 8.2% exhibiting an anonymity set with a size between 2 and 9.

Limitations

This paper shows quality results in its analysis of browser fingerprinting, but does not contribute much in the way of defenses to its explored attack method. In this case, due to the demonstrated results, it is sensible to leave things focused on the attacking side, in addition to reasonably expressing the difficulty of constructing viable defense methods at all; however, there was virtually no novel contribution made on the subject of defense that is capable for the end-user to implement, with the suggestions primarily aimed at browser engineers.

Future Work

As the work focuses on the offensive, there is plenty of room for work in further developing defensive strategies, especially strategies which can be carried out by end-users to place them in control of their own anonymity to untrusted parties. On a similar note, it would be interesting to further abstract and explore the possibility of solidifying a mathematical model aimed at minimizing the effectiveness of the model driving the explained attack.



Feedback to Learner

10/19/18 1:12 AM

Please do a bit more proofreading in the future, there are some pretty obvious typos in the your review

(You’re right... but this was too funny, I couldn’t resist)