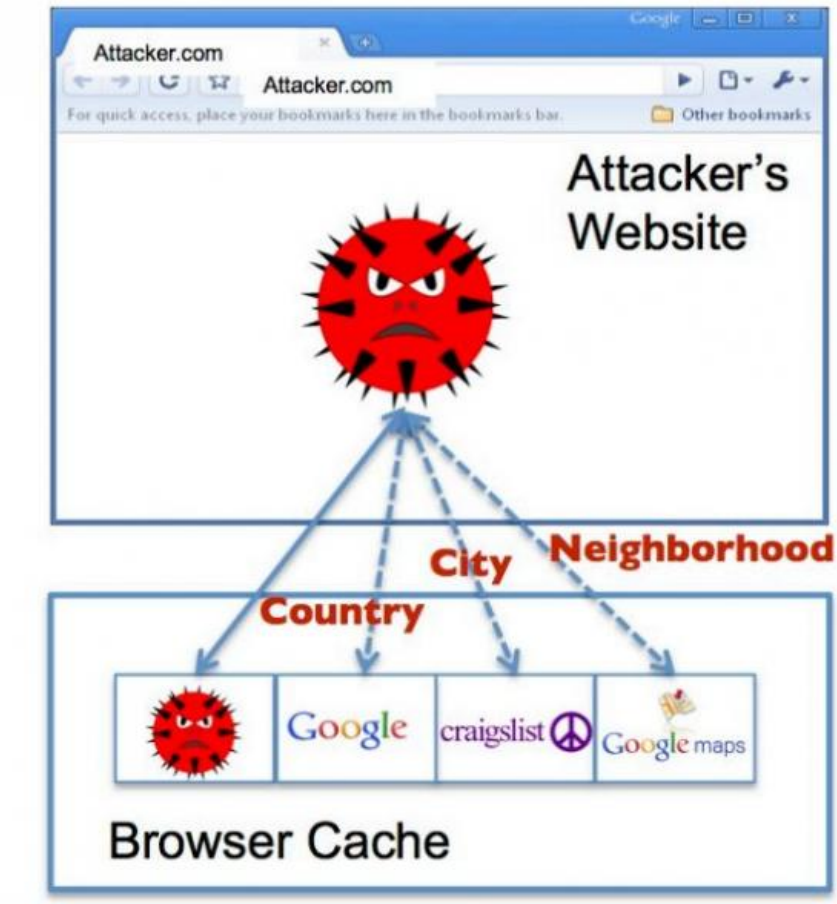
University group reveals geo-inference attack threat that uses browser cache to reveal user location

April 20 2015, by Bob Yirka



Geo-inference attacks sniff location-sensitive resources left by the location-oriented sites (e.g., Google, Craigslist, and Google Maps) through timing side channels in the browser cache to infer the victim's geolocation. Credit: Yaoqi Jia et al.

A team of researchers at the National University of Singapore has published a paper on their university web site outlining what they describe as geo-inference attacks—where hackers can set up a website and then use cache information in a user's browser to reveal their geographical location.

Most Internet users are aware that some websites collect information about them—they see ads for products that are related to sites that they have visited, for example. What most people probably do not realize however, is that data stored on a user's computer by a website, such as Google, can be used to reveal geographical location information to other web sites.

Most sites, including Google, encrypt information they save on a user computer, but hackers, and the team in Singapore have found a way around this. Here is how it works—when you go to Google, Google notes which country you are in by your IP address and then stores that information in your cache so that the next time you go to Google, your computer will not have to download the logo—it can just pull it off your hard drive, which is a lot faster—that makes the Google site appear to load faster. Leaving that logo on your hard-drive presents an opening for hackers, though, because if they can get you to visit their web site (via spam, clicking on a link on another web site, etc.) they can get access to your cache. They cannot read the file Google left there, but they can check to see if the logo is there, Google does not bother scrambling its name.

To figure out which country you are in, all they have to do is attempt to read the logo off your drive three times (to determine if its cached)—and thereby infer your country location. They can do this because they know that Google has 191 regional domains, placed

strategically around the world to provide optimal download speed for visitors to their site. To figure out a user's country, all they have to do is compare the time it takes to download the Google logo (image load time) against all the 191 possibilities—the one that loads the fastest, because it is cached, reveals the country location. Thus, the hackers can infer country location based on data residing in the cache left by another site.

The researchers report that by using a similar approach, hackers can use information left by sites such as Craigslist, Google Maps, etc. to zero in on city, neighborhood, or even street address. They report also that they tested all of the most popular browsers and found them all vulnerable to the same type of attack and claim that 62 percent of the Alexa top 100 websites in the US, Japan, Australia, the UK and Singapore leak location data.

More information: I Know Where You've Been: Geo-Inference Attacks via the Browser Cache, PDF: www.comp.nus.edu.sg/~jiayaoqi/ … ns/geo_inference.pdf