Researchers ID ways to exploit ‘cloud browsers’

North Carolina State University

Researchers from North Carolina State University and the University of Oregon have found a way to exploit cloud-based Web browsers, using them to perform large-scale computing tasks anonymously. The finding has potential ramifications for the security of “cloud browser” services.

At issue are cloud browsers, which create a Web interface in the cloud so that computing is done there rather than on a user’s machine. This is particularly useful for mobile devices, such as smartphones, which have limited computing power.The cloud-computing paradigm pools the computational power and storage of multiple computers, allowing shared resources for multiple users.

“Think of a cloud browser as being just like the browser on your desktop computer, but working entirely in the cloud and providing only the resulting image to your screen,” says Dr. William Enck, an assistant professor of computer science at NC State and co-author of a paper describing the research.

Because these cloud browsers are designed to perform complex functions, the researchers wanted to see if they could be used to perform a series of large-scale computations that had nothing to do with browsing. Specifically, the researchers wanted to determine if they could perform those functions using the “MapReduce” technique developed by Google, which facilitates coordinated computation involving parallel efforts by multiple machines.

The research team knew that coordinating any new series of computations would entail passing large packets of data between different nodes, or cloud browsers. To address this challenge, researchers stored data packets on bit.ly and other URL-shortening sites, and then passed the resulting “links” between various nodes.

Using this technique, the researchers were able to perform standard computation functions using data packets that were 1, 10 and 100 megabytes in size. “It could have been much larger,” Enck says, “but we did not want to be an undue burden on any of the free services we were using.”

“We’ve shown that this can be done,” Enck adds. “And one of the broader ramifications of this is that it could be done anonymously. For instance, a third party could easily abuse these systems, taking the free computational power and using it to crack passwords.”

However, Enck says cloud browsers can protect themselves to some extent by requiring users to create accounts – and then putting limits on how those accounts are used. This would make it easier to detect potential problems.

The paper, “Abusing Cloud-Based Browsers for Fun and Profit,” will be presented

Dec. 6 at the 2012 Annual Computer Security Applications Conference in Orlando, Fla. The paper was co-authored by Vasant Tendulkar and Ashwin Shashidharan, graduate students at NC State, and Joe Pletcher, Ryan Snyder and Dr. Kevin Butler, of the University of Oregon. The research was supported by the National Science Foundation and the U.S. Army Research Office.

Source: http://news.ncsu.edu/releases/wms-enck-cloud-browsers/ [1]

Links:
[1] http://news.ncsu.edu/releases/wms-enck-cloud-browsers/