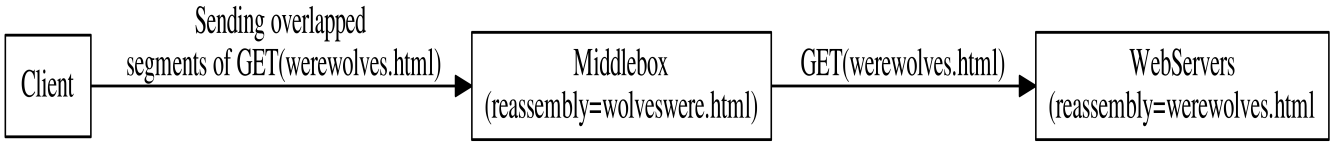
Name: Rajkumar Pandi
Email : cbvpandiraj@gmail.com

Abstract

Generally Internet censorship in a country is performed by some devices that does filtering at granular level. Nowadays, the trend changed where the corporates were believed to be helping the government or were obligated to volunteer for doing censorship in a country. It is a laborious task to differentiate whether censorship is done by the government, the ISP or by the corporate itself, and to verify the complicity between them. In this paper, we propose a approach to exactly identify the “Bozeman” performing the censorship.

The main idea behind is, middle boxes never process or observe traffic as same as the destination host. By sending overlapping IP fragments/ TCP segments, we would able to observe the difference in the reassembly process as different operating system have their own reassembly policy. For example, assume ISP's middle box running FreeBSD, and the web server in a country runs Linux. By sending overlapping fragments/segments of a blocked content in such a way that middle box reassemble the GET request to unblocked content, and the web server in a country reassemble for blocked content. Using this methodology, we can determine who is doing the granular censorship based on the GET request, and also circumvent the censorship. In the above case, if we are able to access the known blocked content from the web server, then we know that middle box is bozeman. After evading the middle box by reassembling the GET request to unblocked content, and still we were unable to access the content reveals that web server is bozeman.



Citizen's lab recent study on censorship practices of popular search engines reveals that these companies maintain a low level of transparency regarding their censorship practices. This project not only used to detect bozeman, but also focuses on emphasizing corporate's social responsibility. This project will provide a tool to verify the corporate compliance with their public pledges as well.