User-side approach for censorship detection: home-router and client-based platforms

Giuseppe Aceto[1], Nick Feamster[2], Antonio Pescapé[1]
[1]University of Napoli "Federico II", Italy [2]Georgia Institute of Technology, USA

Problem statement - Monitoring the occurrence of Internet censorship and identifying the employed techniques are instrumental to scientifically document the phenomenon, detect possible side-effects affecting entities outside the censored network, raise the awareness of the users, and empower them with respect to political decisions. The use of a global-scale network of probes is necessary to exploit the diversity of the censorship events, usually confined in national borders [1,2], and also presenting collateral effects on countries outside the one applying censorship [3,4]. Despite such strong motivations, the study of censorship in many countries has thus far been limited by the possibility to have probes able to perform censorship tests from within the country.

Approaches - Different methods can be adopted to detect censorship: a coarse classification is between server-side and user-side. Server-side detection [5] can reliably monitor usage patterns of offered services on the servers themselves, while user-side detection is performed by trying to access online resources from a client, and can leverage different types of probes (e.g. gateway boxes or user devices). Gateway-based approaches have the advantages of continuous operating times, and are not subject to personal firewalls and application filters; on the down side the deployment of router devices poses logistical problems, and the devices have limited computational and storage resources. Client-based approaches [6] by using applications on user hosts solve some of the issues of the gateway-based approach: the dissemination of the probes on global scale and the availability of computational and storage resources typical of a personal computer; on the other hand detection tests execution is bound to the client uptime, is possibly impaired by network filtering applications, and has to avoid interfering with user QoE. We have explored user-side detection with both these approaches, in the projects BISMark[7] and UBICA[8], benefiting from their advantages while mitigating the respective limitations.

Detection tests - we have implemented on both BISMark and UBICA platforms the censorship detection tests of type Content Blocking, as classified in [6]: HTTPscan (URL retrieval), DNS lookup, keyword-based HTTP filtering; these tests require a list of candidate targets (hostnames, URLs, keywords) that are possibly subject to censorship, and verify their (un-)reachability from the probe. All tests perform active measurements, i.e. no information from user activity or user traffic is collected, avoiding possible concerns about user privacy. The implementation of the tests share most of the code between the two platforms, allowing for direct comparison and merge of the results, that are reported in a common format to allow easy data sharing and reuse.

The presenter will provide a poster describing the architecture of the used platforms, the detection tests implemented and the results of the preliminary deployment.

[1] Internet filtering, 2010. Tech. rep., OpenNet Initiative, 2010.

[2] John-Paul Verkamp and Minaxi Gupta, "Inferring Mechanics of Web Censorship Around the World", Free and Open Communications on the Internet (Bellevue, WA, USA, 2012), USENIX.

[3] Dainotti , A., Squarcella , C., Aben , E., Claffy, kc, Chiesa , M., Russo , M., and Pescape` , A. "Analysis of country-wide Internet outages caused by censorship", In ACM/USENIX Internet Measurement Conference (IMC) (2011).

[4] Anonymous, "The collateral damage of internet censorship by DNS injection," SIGCOMM Comput. Commun. Rev., vol. 42, no. 3., July 2012

[5] Google Transparency Report - Traffic http://www.google.com/transparencyreport/traffic

[6] Arturo Filastò and Jacob Appelbaum, "OONI: Open Observatory of Network Interference", Free and Open Communications on the Internet (Bellevue, WA, USA, 2012), USENIX.

[7] Srikanth Sundaresan, Walter de Donato, Nick Feamster, Renata Teixeira, Sam Crawford, Antonio Pescapè, "Broadband Internet Performance: A View From the Gateway", ACM SIGCOMM 2011.

[8] UBICA project, http://ubica.comics.unina.it