International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Tool and Techniques to Bypass Internet Filtration

Nand Kumar Singh[*1], Brajkishor Pathak[2], Harishankar Prasad Tonde[3]
[*1]Department of Computer Application, Loyola College Kunkuri, Jashpur, Chhattisgarh, India
[2]Department of Computer Application, Loyola College Kunkuri, Jashpur, Chhattisgarh, India
[3]Department of Computer Science(U.T.D.), Sarguja University , Ambikapur, Chhattisgarh, India

ABSTRACT

A key component for any censorship resistant system or circumvention technology is to ensure privacy by enabling users to communicate undetected in a censorship network. This is often accomplished by incorporating certain techniques such as pseudonymity and anonymity into the system. However, previous research suggests that current techniques to ensure privacy still reveal a significant amount of identifying information [1]. In addition to addressing the limitations for ensuring privacy using tools other research has introduces four properties: anonymity ,unlink ability, unobserved ability and pseudonymity, and a set of anonymity metrics, which can be used to improve the design and evaluation of censorship resistant systems [2].

Keywords: Censorship, Network, Technique.

I. INTRODUCTION

This So far the analysis of previous research has identified two main challenges for designing censorship resistant systems. These challenges include research focused on content protection and anonymity to ensure privacy. In addition to content protection and anonymity other approaches for designing censorship resistant systems have centred on issues related to content filtering. Therefore the main technical approaches for addressing challenges with designing censorship resistant systems include:

(1) Anonymity,
(2) Content protection, and
(3) Content filtering.

In addition to the technical approaches and research on censorship resistant systems discussed above, several social and behavioural *methods* have also been investigated. For example, the first economic model of censorship resistance based on conflict theory and node preferences in a peer-to-peer system was presented by Danezis and Anderson (2004)[3].

Many different approaches to design censorship resistant systems have been proposed. The approaches so far have consisted of possible solutions from both technical and social perspectives. A comprehensive and successful Internet censorship strategy involves collaboration and coordination among various social, political and technological entities. Therefore, a solution to Internet censorship must attempt to exploit the vulnerabilities within each entity. A solution to Internet censorship may evolve from a technological perspective provided it is designed with the optimal combination of features including an underlying or indirect motive to destabilize social and political structures.

II. METHODS AND MATERIAL

Several anti-censorship techniques have been developed to circumvent the a fore mentioned technical filtering methods. While there are many academic projects actively engaged in the development of circumvention technologies. The variety of commercial anti-censorship applications is based on one of the following circumvention methods described in **Table 1**[4].

Table 1

Method	Definition
HTTP Proxy	HTTP proxying sends HTTP requests through an intermediate proxying server. A client connecting

	through an HTTP proxy sends exactly the same HTTP request to the proxy as it would send to the destination server unproxied. The HTTP proxy parses the HTTP request; sends its own HTTP request to the ultimate destination server; and then returns the response back to the proxy client
CGI Proxy	CGI proxying uses a script running on a web server to perform the proxying function. A CGI proxy client sends the requested URL embedded within the data portion of an HTTP request to the CGI proxy server. The CGI proxy server pulls the ultimate destination information from the data embedded in the HTTP request, sends out its own HTTP request to the ultimate destination, and then returns the result to the proxy client.
IP Tunnelling	Some of the most common tools used for IP Tunnelling include virtual private networks or VPNs. VPNs give the user client a connection that originates from the VPN host rather than from the location of the client. Thus a client connecting to a VPN in a non-filtered country from a filtered country has access as if he is located in the non-filtered country.
Re-routing	Re-routing systems route data through a series of proxying servers, encrypting the data again at each proxy, so that a given proxy knows at most either where the traffic came from or where it is going to, but not both.
Distributed Hosting	A distributed hosting system mirrors content across a range of participating servers that serve the content out to clients upon request. The primary advantage of a distributed hosting system is that it provides access to the requested data even when the original server cannot, for instance if the original server has been overwhelmed by traffic or even taken down by a denial of service attack

III. CONCLUSION

Proxies provides vastly improved online anonymity, and protects your entire on-line life.

Base	Proxy
Online Security	It gives very low-level security. Only on SSL connection everything is encrypted but on non-SSL connection everything is vulnerable to cyber threats.
Online Privacy	When using a Proxy, anyone can intercept your private data.
Online Freedom	It only works for certain geo-restrictions and cannot help you bypass strong firewalls and censorship.
Speed	It does compromise your internet speed to great extent due to overloaded servers.
Compatibility	It is limited only to certain browsers.
Reliability	Only works for bypassing geo-restricted channels and provides no security at all. Hence, not reliable.

IV. REFERENCES

[1]. J. R.Rao and P.Rohatgi.Can pseudonymity really guarantee privacy? In Proceedings of the Ninth USENIX Security Symposium, pages 85–96.USENIX, Aug.2000.<http://www.usenix.org/publications/library/proceedings/sec2000/full_ papers/rao/rao.pdf>.

[2]. George Danezis and Claudia Diaz.A survey of anonymous communication channels.Technical Report MSRTR-2008-35, Microsoft Research, January 2008.

[3]. George Danezis and Ross Anderson.The economics of censorship resistance.In The Third

Annual Workshop on Economics and Information Security (WEIS04),2004.

[4]. Roberts et al,"2007 Circumvention Landscape Report: Methods, Uses, and Tools," The Berkman Center for Internet & Society at Harvard University, March 2009