2008

Subverting National Internet Censorship - An Investigation into existing Tools and Techniques

Jason Smart
Edith Cowan University

Kyle Tedeschi
Edith Cowan University

Daniel Meakins
Edith Cowan University

Peter Hannay
Edith Cowan University

Christopher Bolan
Edith Cowan University

DOI: 10.4225/75/57b275c540cc1
Originally published in the Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

Subverting National Internet Censorship - An Investigation into existing Tools and Techniques

Jason Smart, Kyle Tedeschi, Daniel Meakins, Peter Hannay & Christopher Bolan
School of Computer and Information Science
Edith Cowan University

Abstract

The announcement of a trial of a National level internet filter in Australia has caused renewed interest in the arena of internet censorship. Whilst details on the schemes being tested have been fairly sparse the announcement of the trial itself, has drawn wide condemnation from privacy advocates throughout the world. Given this announcement it was decided to test and compare three of the most popular free tools available that allow for the bypassing of internet censorship devices such as those used within China. Tests were conducted using three software packages, Freegate, GPass and GTunnel which were analysed through packet capture to determine their likely effectiveness against the speculated methods to be employed by the Australian trials. The tests clearly showed that all three applications provide an easy means of subverting any likely filtering method with GPass and GTunnel the more suitable candidates as Freegate still allowed for plain-text DNS requests.

Keywords

Censorship, Gpass, Gtunnel, FreeGate, filtering, internet filtering, government censorship, bypass filtering

INTRODUCTION

Internet censorship in Australia is governed by a tangle of laws and regulation at both Federal and State/Territory level which is attributable to the lack of censorship and control powers granted to the Government in the Australian Constitution (EFA, 2008). Specifically the current legislation is focused as follows (*ibid)*:

- Commonwealth Level - focused on Internet Content Hosts (ICH) and Internet Service Providers (ISP), but no regulation is specified for content creators or end users. This level of legislation allows powers for the Government or an appointed regulator to order providers and hosts to remove hosted content that is deemed "objectionable" or "unsuitable for minors".
- State / Teritory Level – focused on both ISPs/ICH and user level and differs from state to state and often allow for the prosecution of users for "making available" material that is deemed by legislation to be "objectionable". Beyond this some jurisdictions also apply a penalty for the viewing or downloading of such content.

Recently, it has been noted that "[Australia's] net censorship laws are more akin to those in totalitarian regimes than to those, if any, in other countries purporting to be Western democracies" (Libertus, 2008). Such claims are backed by Electronic Frontiers Australia who charge that "following extensive criticism by EFA and other organisations and individuals, it [Australian censorship] remains a draconian scheme unlike any existing or proposed laws in countries similar to Australia" (EFA, 2008). Whilst this issue may be seen as a relatively new reaction to the announced plans of the Federal Government (Marshall, 2008), a lot of the issues seen today relate back to the amendment of the Freedom of Information Act in 2003 (Comlaw, 2008). Whilst claiming to assist in the removal of objectionable content on the internet the result of the bill was to grant the government wider and unilateral powers in what could be deemed "objectionable" (EFA, 2008).

As alluded to early the current plans of the Federal Government to trial and eventually impose mandatory content filtering at the ISP level has drawn a wide rage of criticism and concern (Dudley-Nicholson, 2008; EFA, 2008; Libertus, 2008). With such concerns abounding it seemed to be an apposite time to explore and contrast freely available tools used to bypass internet censorship regimes in other countries and investigate their usefulness and speculate on their effectiveness against future Australian filtering schemes.

SELECTION OF FILTER BYPASS SOFTWARE

To carry out this investigation it was decided to select three of the most popular freely available programs that allowed for the bypassing internet content filters (Global Internet Freedom [GIF], 2008). The three chosen software applications were GTunnel, FreeGate and GPass, each of which functions in a slightly different

manner, using different infrastructure or methods of bypassing internet content filters (GPass, 2008; Garden Networks, 2008; Dynamic Internet Technologies, 2008).

GPass

GPass is an anti-censorship application created by The World's Gate Inc designed to bypass censorship methods used to filter out internet content (GPass, 2008). Initially released in July 2006, GPass is now one of the five most used anti-censorship tools and to date is also only one of two (the other being FirePhoenix) that claim to offer multi-protocol support such as Web 2.0, online multimedia, and communication tools such as email and instant messaging (Wang, 2008). According to its producers, GPass is able to bypass censorship devices such as the Chinese Great Firewall allowing anonymous web surfing whilst protecting the users identity and encrypting Internet communication, utilising a proprietary method to find an available server from the GPass server farm and then establishes an encrypted tunnel on the other side of the censorship firewall (GPass, 2008). The operation of GPass is illustrated below in figure 1.

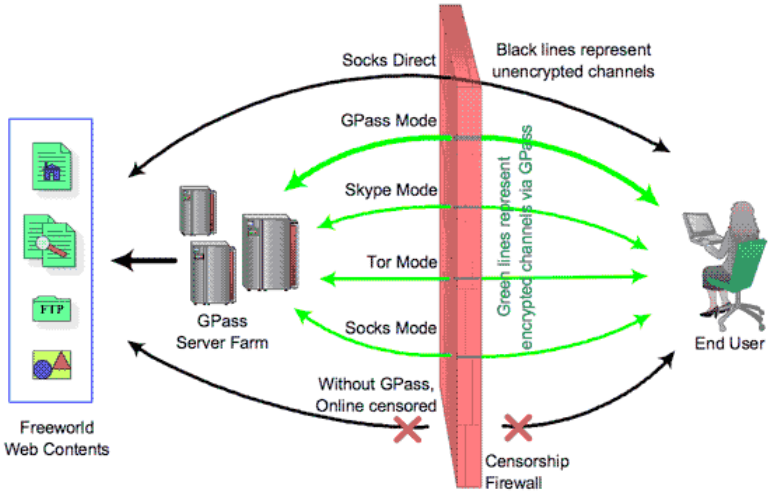

Figure 1. Overview of GPass Operation (GPass, 2008)

GTunnel

The second toll selected for the investigation was GTunnel designed by Garden Networks for Freedom of Information, a small development house based Canada (Garden Networks, 2008). The creators of the GTunnel software claim to have created the Garden Network and its front-end application, GTunnel, to provide users with anonymity while browsing the internet (*ibid*). GTunnel functions by providing a local SOCKS v5 or HTTP proxy on the host computer, which facilitates a connection to the Garden Networks server farm, the proxy is then automatically configured inside Microsoft Internet Explorer, which will send all browsing traffic through the secure proxy tunnel thus obfuscating the host computer IP address and anonymising http traffic. GTunnel operates in two modes of operation, namely TOR based and Skype based. These options effect the network used to first make the connection, in both cases the connections pass through GTunnel's own servers prior to reaching its destination. In order to understand the consequences of each of these methods a brief introduction to the Skype and TOR networks is required.

TOR operates by routing encrypted data through a series of TOR nodes, each of these nodes is operated by volunteers who wish to support (or undermine) the TOR network (Bugher, 2007). The last TOR node before the traffic continues out to it's final destination is known as an 'exit node' the exit node is special in that it sees the traffic in the format intended to be received by the destination, this can often be unencrypted and insecure, whilst all the other nodes will only see encrypted data (*ibid*). The concept of a hostile exit node is nothing new and has in the past been used to intercept email and other passwords (Gray, 2007), GTunnel addresses the issue of hostile exit nodes by using its own servers as an encrypted proxy between TOR and the intended destination (Garden Networks, 2008).

This however does not eliminate the risk associated with hostile exit nodes, it merely shifts the trust to another party, in this case Garden Networks. Skype is a peer to peer (P2P) based voice over IP (VOIP) service that is built specifically to bypass firewalls so that customers can make calls regardless of the filtering mechanisms in place (Schmidt, 2006). GTunnel uses an unknown method to make use of the Skype network in order to bypass

content filtering networks, it should be noted that Skype makes use of encryption methods that should make decoding of data whilst it is within the Skype network unfeasible (Baset & Schulzrinne, 2004).

In each of these cases Garden Networks is trusted to respect its users privacy as it is able to intercept unencrypted data passing through it's network. However the use of the TOR mode of operation should prevent Garden Networks from determining the origin of this data (this is assuming that the unencrypted data itself does not provide this information).

FreeGate

The final application, Freegate is an anti-censorship program designed by Dynamic Internet Technology (DIT-US), for use in countries where internet censorship occurs (Dynamic Internet Technologies, 2008). Dynamic Internet Technology has a strong affiliation with the United States Department of Defence for whom they created Dynaweb on which the Freegate application is based (*ibid*). The software claims to be a secure and fast way of browsing the internet in relative security having the added feature of not requiring installation on the user's system and working without altering the host computers system settings (GIF, 2008). Freegate has two separate modes one to run in proxy mode, in which it automatically sets the IE proxy settings, the other defaults to Dynaweb servers overseas where you can browse websites straight through the mirror however this option limits its multi-protocol support (Dynamic Internet Technologies, 2008). It is claimed by Dynamic Internet Technologies that due to its method of bypass that, any program that is capable of using the SOCKS v5 proxy is capable of using Freegate to hide its traffic (*ibid*).

TEST SETUP

In order to provide a suitable testing framework, virtual machines were used to ensure that the test environment remained consistent and clean throughout. The host system was running VMware Server 1.0.6 on a Windows XP SP3 system. Two identical virtual machines were created which were running Windows XP SP3 and the following applications as well as the tool being tested:

- Internet Explorer 7,
- Mozilla Firefox 3,
- VMware Tools 7.6.2,
- uTorrent 1.8,
- FileZilla Client 3.1.1.8,
- Xchat 2.8.7c,
- Windows Live Messenger 8.5.1302.1018,
- Google Talk 1.0.0.104,

VMware was configured to have only a host based virtual NIC. Therefore, the virtual NIC on the host machine acted as the gateway for the virtual machine. IP routing was then enabled on the Windows XP host system to allow Internet access to the virtual machine and Wireshark was installed on the host which was then used to capture packets originating from the VMware Virtual NIC thus ensuring all packets would be captured by the experiment. The setup is illustrated in figure 2 below.

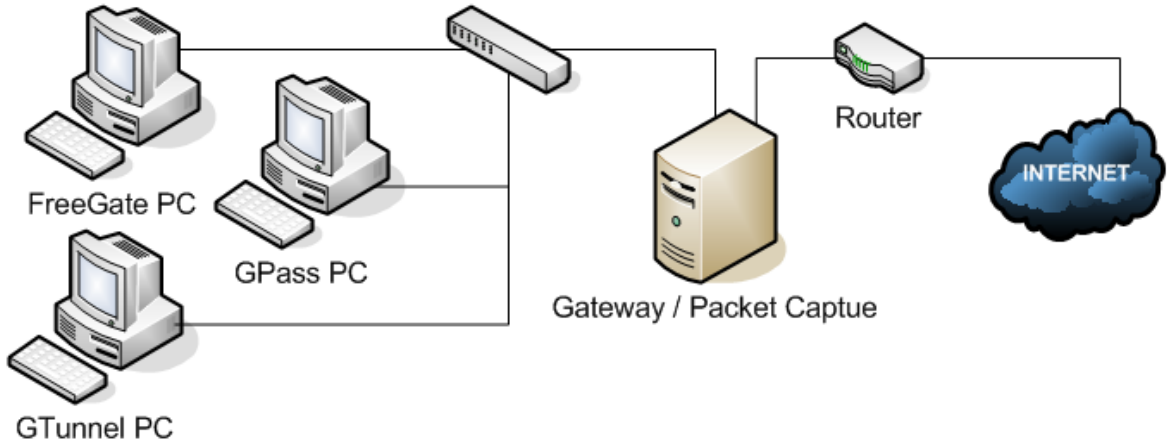

Figure 2. Experimental Setup for Testing

Before the testing was undertaken, a baseline of results were created using the same setup without the Bypass software application in order to allow an easy determination of the effects of the anti-censorship tool. Subsequently the experiments were conducted using the default setups for each application. Upon completion, these tests were then compared with the baseline tests using Wireshark 0.99.8 (Combs, 2008) and NetworkMiner 0.85 (Hjelmvik, 2008) to analyse the packet dumps and extract relevant information.

RESULTS

The results of each test were recorded in order to allow the software applications to be compared to each other and to the baseline in order to determine the effectiveness of these tools for the obsfucation of various protocols.

Table 1. Results of Testing

	Gpass	**FreeGate**	**Gtunnel**	**No Bypass Software**
Webmail	Hidden	Hidden	Hidden	Plaintext
POP3	Hidden	Hidden	Hidden	Plaintext
SMTP	Unknown*	Unknown*	Unknown*	Plaintext
Google Talk	Hidden	Hidden	Plaintext/Hidden**	Plaintext/Hidden**
Windows Live Messenger	Hidden	Hidden	Plaintext	Plaintext
IRC	Hidden	Hidden	Hidden	Plaintext
HTTP	Hidden	Hidden	Hidden	Plaintext
HTTPS	Hidden	Hidden	Hidden	Plaintext
FTP	Hidden	Hidden	Hidden	Plaintext
BitTorrent	Hidden	Hidden	Hidden	Plaintext

* Unable to be tested as none of the clients properly supported SOCKS

** Conversations were hidden whilst protocol messages were not

The results of testing are shown in Table 1 above, in each case the result of the test is listed as hidden or plaintext. Hidden specifies that the contents of the packets as shown in Wireshark and Network Miner appear as encrypted or otherwise obsfucated traffic. It should be noted that in every case where traffic was hidden in some way the protocol used appears to be SSLv3, this protocol is believed to be secure as long as the private certificate of the server is not known. If the private certificate is known it is possible to decrypt all traffic sent to and from the server in question. It may be seen that GPass and FreeGate are able to hide Google Talk and Windows Live Messenger whist GTunnel does not support these protocols. In each of the other tests all three solutions were able to hide the data sent across the network in the method specified. In each case the operational

mode of the software (for example, TOR or Skype) had no impact the effectiveness of the software in any observable way.

Aside from the observations presented in Table 1, it should be noted that FreeGate sends all DNS requests in plaintext across the network. It also makes use of the US Department of Defence (DoD) DNS servers, this may prove to be a security risk as the US DoD or any host in position to intercept traffic between the source and destination of these DNS requsts could determine the exact IP address of the computer originating the request as well as the details of the requested domain name. It is conceivable that this would render FreeGate to be unsuitable for bypassing some content filtering mechanisms if these track DNS requests to determine if illict content is being accessed.

Table 2. Methods of bypassing different content filtering methods

Content Filtering Method	Filtering Bypass Method
Filtering DNS requests	Route DNS requests though an encrypted tunnel
Filtering Web page contents	Route web traffic through an encrypted tunnel
Filtering IP addresses	Route all traffic through an encrypted tunnel

In order to evaluate each of the tools usage in terms of bypassing internet content filtering, it is first important to understand how each of these content filtering methods function. There are three main types of internet content filtering, these are, filtering DNS requests, filtering web page content and filtering IP addresses. In each of these cases there is a different method of bypassing these restrictions. These filtering methods and their corresponding bypass methods are presented in Table 2.

Table 3. Results of testing bypass tools against defined bypass methods

	GPass	**GTunnel**	**FreeGate**
Route DNS requests though an encrypted tunnel	Supported	Supported	Not Supported
Route web traffic through an encrypted tunnel	Supported	Supported	Supported
Route all traffic through an encrypted tunnel	Supported	Supported	Supported

The evaluation of each tool to determine which methods of content filtering is supported was conducted and the results displayed in Table 3. These results show that both GPass and GTunnel support all the defined methods for the bypassing of internet content filters, however FreeGate sends all DNS requests openly through the internet and as such it would be possible for a third party determine the domain names on which content may have been retrieved, but not the details of which content was retrieved as this is encrypted. It would also be possible for a content filtering system to intercept and block DNS requests for domains which are considered to be objectionable or otherwise undesirable by the governing body controlling the filtering system. Based on this analysis it can be seen that both GPass and GTunnel would allow for content filtering to be bypassed entirely, however FreeGate does not meet the DNS tunnelling requirement and as such may be unsuitable for accessing prohibited content when behind an internet content filtering system.

CONCLUSION

As outlined in this paper, there is an ever increasing trend in Australia towards draconian internet censorship and the latest moves by the Australian Federal Government to trial filtering methods at the ISP levels is another chip in the ever eroding idea on free speech on the net. Yet despite the claims of the Government that such measures will make the Internet safter, it would seem that anyone with a rudimentary knowledge of search engines would be able to locate free software to bypass such censorship.

This study has found that three of the most popular free tools for ensuring internet privacy and bypassing censorship firewalls would likely function well against likely measures taken at the ISP level. This finding brings into question the need for such filtering, if the method for bypass is so simple and would actually make

the detection of illegal activity from packet capture that much more difficult. Whilst it is easy to tout filtering measures as a ‘cure’ for objectionable material it will have little or no real effect on the access of such materials inside Australia to any but the most naive of users and will likely result in a degrading of the service speeds currently available to Australian internet users.

Unfortunately, despite an initial outcry about the testing of these measures there has been little pressure put on the Government from the general public. One has to wonder whether the public will ever stand up to such inroads into blanket censorship or sit quietly as Australia joins the list of censored nations taking its place with China Iran, and Syria.

REFERENCES

Baset, S., & Schulzrinne, H. (2004). An Analysis of the Skype Peer-to-Peer Internel Telephony Protocol. *Arxiv preprint cs.NI/0412017*.

Bugher, G. (2007, December 10th). Anonymity with TOR and its limits Retrieved November 4th, 2008, from http://perimetergrid.com/wp/2007/12/10/anonymity-with-tor-and-its-limits/

Combs, G. (2008). Wireshark (Version 0.99.8).

ComLaw (2002). Communications Legislation Amendment Bill (No. 1), from http://www.comlaw.gov.au/ComLaw/Legislation/Bills1.nsf/0/011C0CDFB2CA36BECA256F7200246D3E?OpenDocument&VIEWCAT=item&COUNT=999&START=1

Dudley-Nicholson, J. (2008). Australia's compulsory internet filtering 'costly, ineffective', from http://www.news.com.au/technology/story/0,25642,24569656-5014239,00.html

Dynamic Internet Technologies (2008). Freegate, from http://www.dit-inc.us/freegate

EFA (2008). Internet Censorship Laws in Australia, from http://www.efa.org.au/Issues/Censor/cens1.html

Garden Networks (2008). Garden Networks for Freedom of Information, from http://gardennetworks.org/

Global Internet Freedom [GIF] (2008). Global Internet Freedom Consortium – Our Solutions, from http://www.internetfreedom.org/Products-and-Services

GPass (2008). Global Pass Home Page, from http://gpass1.com/gpass/about

Gray, P. (2007, November 13th). The hack of the year Retrieved November 5th, 2008, from http://www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html

Hjelmvik, E. (2008). NetworkMiner (Version 0.8.5).

Libertus (2008). Australia's Internet Censorship System, from http://libertus.net/censor/netcensor.html

Marshall, T. (2008). Minister welcomes advances in internet filtering technology, from http://www.minister.dbcde.gov.au/media/media_releases/2008/060

Schmidt, J. (2006, 15 December 2006). The hole trick - How Skype & Co. get round firewalls Retrieved November 6th, 2008, from http://www.heise-online.co.uk/security/How-Skype-Co-get-round-firewalls--/features/82481

COPYRIGHT