Freegate: A Defence against the Pending Censorship of Australia?

C. Bolan and P. Hannay

School of Computer and Information Science
Edith Cowan University
e-mail: c.bolan@ecu.edu.au; p.hannay@ecu.edu.au

Abstract

The commencement of a trial of Internet Service Provider (ISP) level content filtering as a precursor to nation-wide mandatory content filters in Australia has generated a large amount of publicity. Despite remaining low on details, figures released show that the laboratory testing of the filtering solutions caused significant slow-down in Internet speeds as well as the unintentional censorship of allowable content. This paper investigates the currently available information on the trials and provides evidence that a freely available privacy tool such as Freegate could be used to bypass all of the likely filtering methods.

Keywords

Censorship, Content Filtering, Encryption, Freegate

1. Introduction

Since the passage of laws in 1995 allowing for the Internet to be included under existing censorship legislation, the issue of Internet censorship has grown to become a troublesome issue for governments worldwide (EFA, 2009). Globally organisations such as Electronic Frontier Foundation (EFF) and the Electronic Frontiers Australia (EFA) are being created to monitor and inform the public on censorship issues (EFF, 2009). According to these organisations the current level of censorship may be split into four major categories (EFA, 2009):

1. Government encouraged self-regulation
2. Criminal law penalties for inappropriate content
3. Government mandated blocking of access to content
4. Government prohibition of public access to the Internet

In the Australian context, Internet censorship is governed by a tangle of laws and regulation at both Federal and State/Territory level which, in part, is attributable to the lack of censorship and control powers granted to the Government in the Australian Constitution (EFA, 2009). 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 / Territory Level – focused on both ISP's/ICH and user level, differing from state to state and often allowing for the prosecution of users for the crime of "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.

The recent start of trials by the Australian Federal Government of a mandatory content filtering at the ISP level has drawn a wide rage of criticism and concern (Dudley-Nicholson, 2008; EFA, 2008; Libertus, 2008). With the results of this ongoing trial sealed despite the large amount of public interest, it is an appropriate time to discuss the potential methods that such filtering may employ, its impact and whether or not the free privacy toolsets such as that supplied by Freegate would likely bypass any methods employed at an ISP level.

2. Current and Proposed Internet Censorship in Australia

Currently, Australia is subject to Internet regulation as defined by the Broadcasting Services Act (1992) whereby ISPs and other providers are prevented from hosting material deemed prohibited. This is in addition to criminal laws which make the accessing, storage or transmission of materials relating to child abuse and sex crimes illegal with a range of penalties attached. The amendment of the Freedom of Information Act in 2003 (Comlaw, 2008) adds to this with its stated purpose, to assist in the removal of objectionable content on the Internet. The actual result of this bill has been to grant the government wider and unilateral powers in what may be deemed "objectionable" content (EFA, 2008).

With the election of the Rudd Government in 2007 a pledge was made to commit 125.8 million dollars over a four year period to cyber safety initiatives including Internet filtering, increased education and expansion of branches of the Australian Federal Police to tackle cyber predation (Conroy, 2008). Of these approaches, it is the ISP level Internet filtering that is causing a stir amongst the anti-censorship groups in Australia. Libertus (2008) notes that "[Australia's proposed] net censorship laws are more akin to those in totalitarian regimes than to those, if any, in other countries purporting to be Western democracies". This is backed by the EFA who advise "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).

Initially the Australian government touted a 'Two-Tier' approach, stating that Australians would be able to opt-out of the filtering and thus have access to an

unfiltered feed to the Internet (Bryant, 2008). Since this statement it has come to light that the 'opt-out' option would still have "illegal" content removed whilst the standard filter feed would be "children safe" (Timmer, 2008). Whilst on the basis that it would be only "illegal" content, some would support this scheme the worries about the filtering scheme are increased by the scarcity of details on how such a scheme is being implemented and how will materials be determined to be "illegal" (Moses, 2008). Further, recent leaks of the "illegal" list have shown that the current list already contains sites that should, under Australian law, be allowable. The inclusion of such legal material in the filtering scheme places the government in a role where it becomes responsible for determining what is moral or acceptable for the population, regardless of the legal status of such material. As such, bypassing the proposed filter and accessing 'inappropriate content' may not necessarily represent legal complications for the user but rather raises an ethical concern for the individual versus those of the current governing bodies.

The initial trials carried out by the Australian Communications and Media Authority (ACMA) were hailed a success by the Australian Federal Government. However, it is salient to note that the only concrete positive statement made by the ACMA themselves about the trials is that "ISP filtering products have developed in their performance and effectiveness since they were last assessed in 2005" (Timmer, 2008). This is in stark contrast to the general findings of the report (ACMA, 2008) which found that five of the six filters that were tested, degraded network performance by over 20 percent, and two of the six resulted in a drop of throughput by more than 75 percent. In addition around half the products trialled allowed more than five percent of the blacklist sites through without any bypass measures and all tests had measurable percentages of false positives.

Such findings are even more striking when it is revealed that only web traffic was targeted and that FTP, P2P and other protocols were all left unimpeded (Moses, 2008). Given the lack of testing on alternative protocols it would be simple to assume that such traffic would be beyond the scope of any current implementation of government mandated ISP filtering. However, according to Ramadge (2008) the Minister in charge of this initiative Senator Stephen Conroy announced on his blog that peer-to-peer traffic would be included in the filtered content when the live trial started in 2009.

Despite such issues ISPs were invited to apply to participate in the first live trial of this scheme in late 2008 and many ISPs including the three largest in Australia namely Telstra, iiNet and Optus submitted applications despite publicising their reservations on the technology (*ibid*). When the announcement of participants was made in February 2009, with the selection of "Primus Telecommunications, Tech 2U, Webshield, OMNIconnect, Netforce and Highway 1" (Marshall, 2009), it was noted by many that all of these companies besides Primus are small players in the ISP market (Sweeney, 2009). Its still is currently unknown when or if the results of these trials will be made publicly available or if as stated the trials will actually end in April 2009.

3. Freegate's ability to hide traffic

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). When used correctly, Dynamic Internet Technologies claims 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*). Freegates operations is illustrated below in Figure 1.

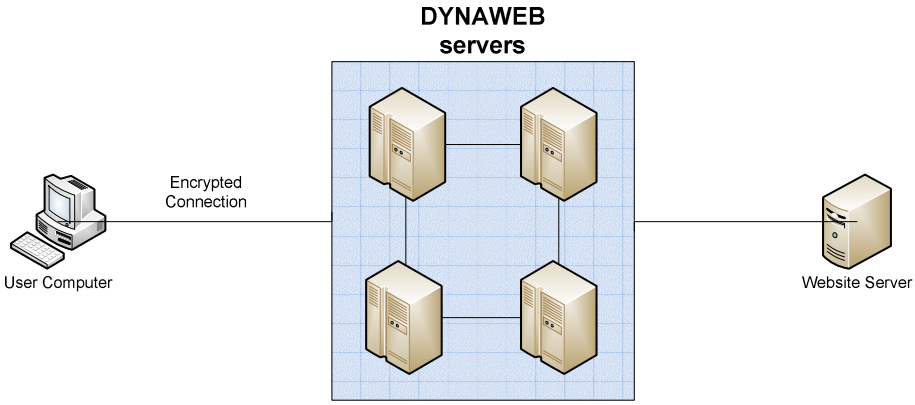

Figure 1 – How Freegate Operates

As the details on the filtering currently being trialled by the ISPs in Australia have not been released the testing was designed to verify if the use of Freegate would hide the traffic generated by the test computer and if so how, and then extrapolate what type of filtering measures such a product would circumvent. In order to provide a suitable framework for this the environment was designed to use several computers running virtual machines to ensure that scenarios were all tested in a clean environment. Every host box was running Windows XP Service Pack 3 with VMware Server Edition 1.0.6 and the Virtual Machines were setup to run Windows XP Service Pack 3 with the following packages installed: Internet Explorer 7, Mozilla Firefox 3, uTorrent 1.8, X-chat 2.8.7c, Mozilla Thunderbird, FileZilla Client 3.1.1.8, Google Talk 1.0.0.104, Microsoft Outlook Express and Freegate 6.76. The use of virtual machines allowed the packets to be transferred between a virtual network card and the host computers network card, before been allowed to travel out

through the gateway on to the Internet. The packets were captured using Wireshark and analysed using NetworkMiner and Interceptor (Combs, 2008; Hjelmvik, 2008).

Freegate has the ability to support the FTP protocol and although the filtering trial specifically excluded FTP traffic it was decided to test this feature as future upgrades could well expand to such protocols. In the tests showed that whilst Freegate's setup made FTP connections more difficult once connected the FTP transfer speed was only slightly degraded from that of normal and that whilst packets and IP's were captured the raw information that was sent could not be recovered. This contrasts with normal whereby without Freegate operating the actual raw files that were downloaded were able to be fully recovered from the traffic.

For the tests of standard web HTTP traffic it was found that as expected normal requests and responses from Internet explorer resulted in the recovery of almost complete information with the website addresses, images and textual content all available from the traffic captured from the test machine. However upon activation of the Freegate program DNS requests were encapsulated in an SSL packet making them unreadable and undetectable. In addition the NetworkMiner software was unable to capture any images or usable text from the traffic. Thus if the ISP filtering had been active and employed packet analysis the Freegate software would have been able to bypass it without any difficulty. The only detectable traffic from the test computer seemed to lead to a server located in Toronto, Canada whose content would not register as inappropriate or 'illegal'.

In response to the claims by Ramadage (2008) peer to peer testing was conducted through the torrent client uTorrent 1.8 (uTorrent, 2008). During the analysis of standard traffic when Freegate was inactive the hosts and DNS requests were easily determinable and the entire file downloaded by this method was also able to be recreated from the packets. Thus, if the new filter targeted such packets it would be able to filter out either all traffic of this kind or block the sharing of specific files or file types. When Freegate was run there will still a large amount of recoverable host and DNS requests, however, the recreation of the file being downloaded proved impossible thus it would be subject to filtering based on the hosts being connected to but not by what was actually being downloaded. Given that the peer the peer swarm is constantly shifting this would mean that either large amounts of hosts (everyone who tried using bittorrent) would have to be filtered out or that such traffic would need to be left alone.

The next area of investigation was the applicability of filtering chat based traffic to this end several tests were run using both IRC as well as instant messaging in the form of Google Talk. The first test of IRC was completed using the IRC program X-Chat and Freegate not in operation. With this setup all the Host computers of people on the channel were viewable, including the names and other server information, beyond this the conversation within the channels were completely viewable from the packet capture. When Freegate was activated only a limited subset of the host servers and the Freegate server (65.49.2.221) were detected, further the packets no longer contained the clear text of the conversation. Similarly to the findings with the bit

torrent peer to peer software it would be possible to block certain hosts using an ISP filter but not filter based on the content of the conversations.

Google talk uses the Jabber protocol, testing in this scenario involved signing on to the client and a standard conversation between clients. The results in these tests were almost identical to the IRC findings with client, host servers and DNS requests all viewable along with some parts of the conversation, whereas with Freegate running all information was encrypted, with no DNS requests found and only 13 hosts discovered compared to 26 with no tunnelling implemented. Thus, again it would be possible to block certain hosts using an ISP filter but not filter based on the content of the conversations.

Finally a range of tests were conducted on email protocols to determine the efficacy of email content filtering when Freegate was employed. The first protocol tests were that of the Post Office Protocol 3. POP3 is one of the most used email protocols today with modern email clients and servers employing this protocol to store the messages on a server until the client downloads them to a local disk via a client such as Outlook Express. When analysed the traffic generated by POP3 using both Mozilla Thunderbird and Microsoft Outlook Express (default mail client for Windows XP) an analysis on the packet dump showed that the email could be read in clear text by following the TCP stream in wireshark when Freegate was not enabled along with all server information and attached files. Once activated Freegate successfully hid both server and message content suggesting that Freegate would bypass both packet and content filtering methods.

Next Simple Mail Transfer Protocol (SMTP) was investigated as SMTP is typically used by large ISP to send emails. To ensure consistency both Mozilla Thunderbird and Microsoft Outlook Express clients were used in the tests but whilst the SMTP operated successfully when Freegate was disabled the clients were unable to connect due to port issues when Freegate was utilised. Upon further investigation it was found that the SMTP server used port 25 whereas Freegate fixes the port on start up automatically in the case of the tests this was to port 8580. Given this it is almost certain that Freegate would not provide any protection against ISP filtering although this might be fixed in future versions of the software.

The final email tests were completed using free online clients such as GMail Google's free Internet mail site and Microsoft Hotmail. Again the test results show that without Freegate 31 DNS requests occurred and were visible along with the 18 servers that were connected to during the session. It also showed that 22 files were recorded, however all were encrypted and unreadable. Further, attempts to follow the TCP streams of the files only turned up more encrypted information with most clear text recorded in the packets referring to their host server. Thus, even without Freegate enabled, the content of the GMail system would likely be difficult to filter in real-time. With Freegate enabled only 2 hosts were connected to, compared to the 18 without and a comparison of the TCP streams showed that all files were encrypted using SSLv3 and that any server information that was previously recorded in the clear traffic packets was now hidden suggesting that should GMail's internal

measure be subverted to allow live filtering Freegate would likely provide a work around.

Likewise Hotmail tests also showed the potential of Freegate in bypassing ISP based content filtering. However unlike GMail, Hotmail was found to not use encryption as a default and thus with packets analysis, NetworkMiner was able to recreate the majority of images and text, as well as several DNS requests and Host server IP addresses. Upon activation Freegate caused some issues with the Hotmail web client allowing the receipt of emails but preventing any sending of content. This was likely due to similar port issues as those found in the SMTP tests but where content was received it had been successfully obfuscated.

4. Conclusion

As this paper has detailed, there has been a steady march towards mandatory Internet filtering in the Australian Internet market. The current trial of ISP level filtering whilst light on details would likely need to employ packet content analysis to be at all effective in filtering out objectionable or illegal content. The currently available reports show that despite Government claims of success, that the trialled approaches filter out a range of legal and allowable content as a by-product, as well as slowing down the average speed of Internet services by as much as 75%.

To make such drawbacks acceptable, the argument is made that the measures will prevent access to illicit or objectionable material and thus are worth any negative side-effects. From the analysis of the content captured without the use of censorship prevention software such as Freegate it seems that filtering would likely work as intended not only against standard web traffic but also additional protocols such as those employed by FTP, and Peer to Peer traffic. In addition messages sent through a variety email and chat clients could also be filtered and blocked.

However it is likely that those individuals who would knowingly access such content would employ a method of bypass such as the anti-censorship package Freegate and thereby could possibly to bypass many if not all filtering techniques based on IP or DNS addresses and packet content. These methods represent the most likely technologies for this level of filter and thus would mean that an individual wishing to access filtered content would still be able to do so without difficulty.

Given the ease by which these methods of filtering may be circumvented the real effect of such filtering would be a slowdown of already poor Internet speeds especially in remote areas and the possibility that legal enterprises may be hampered due to unforeseen filtering of allowable content. Beyond this, it would be foreseeable that the detection of illegal traffic would be made less likely if even a small percentage of the general populace were forced to encrypt all web traffic to enjoy the same Internet freedom as those in other non censored countries.

5. References

ACMA. (2008), *Closed Environment Testing of ISP-Level Internet Content Filtering*. Melbourne, Australia: Australian Communications and Media Authority

Broadcasting Services Act, C2009C00085 (1992).

Bryant, N. (2008), "Australia trials national net filters", http://news.bbc.co.uk/2/hi/technology/7689964.stm, (Accessed 25 April 2009)

Conroy, S. (2008), Internet Filtering. In C. Bolan (Ed.) (pp. 4).

Dudley-Nicholson, J. (2008), "Australia's compulsory Internet filtering 'costly, ineffective'", http://www.news.com.au/technology/story/0,25642,24569656-5014239,00.html , (Accessed 25 April 2009)

Dynamic Internet Technologies. (2008), "Freegate", http://www.dit-inc.us/freegate , (Accessed 25 April 2009)

EFA. (2009), "Electronic Frontier Foundation", http:\\eff.org\, (Accessed 25 April 2009)

EFA. (2009), "Internet Censorship Laws Worldwide", http://www.efa.org.au/Issues/Censor/cens1.html, (Accessed 25 April 2009)

Global Internet Freedom [GIF], (2008), "Global Internet Freedom Consortium – Our Solutions", http://www.Internetfreedom.org/Products-and-Services, (Accessed 25 April 2009)

Libertus. (2008), "Australia's Internet Censorship System", http://libertus.net/censor/netcensor.html, (Accessed 25 April 2009)

Marshall, T. (2009), "Pilot to assess technical feasibility of ISP filtering", http://www.minister.dbcde.gov.au/media/media_releases/2009/005, (Accessed 25 April 2009)

Moses, A. (2008), "Filtering out the fury: how government tried to gag web censor critics", http://www.theage.com.au/news/technology/biztech/how-government-tried-to-gag-censor-critics/, (Accessed 25 April 2009)

Ramadge, A. (2008), "Internet filtering plan may extend to peer-to-peer traffic, says Stephen Conroy", http://www.news.com.au/technology/story/0,28348,24833959-5014239,00.html, (Accessed 25 April 2009)

Sweeney, P. (2009), "ISP filtering pilot goes ahead", http://whirlpool.net.au/news/?id=1834, (Accessed 25 April 2009)

Timmer, J. (2008). "Aussie govt: Don't criticize our (terrible) 'Net filters", http://arstechnica.com/tech-policy/news/2008/10/aussie-govt-dont-criticize-our-terrible-net-filters.ars, (Accessed 25 April 2009)

UTorrent. (2009), "UTorrent: A Very Tiny Bittorrent Client" (Version 1.8)