The Practice of Global Internet Filtering

Pavel Ocenasek

Brno University of Technology, Faculty of Information Technology, Brno, Czech Republic
ocenaspa@fit.vutbr.cz

Abstract. This paper deals with Global Internet Filtering.. Various technical solutions for Internet filtering are presented together with filtering analysis options. Several possibilities for blocked content access and filtering circumvention in general are discussed.

Keywords: Internet filtering, filtering circumvention, surveillance, blocking, firewall .

1 Introduction

The expansion of the Internet let many people access very useful information without any limitations. But the Internet itself does not contain relevant and useful information only. It's available to everybody without any difference and it's not possible to prevent users from becoming the victims of malicious behavior of the other users. The need for controlling the way people use the Internet is based on all the positives and negatives that the Internet has adopted over the years from the real world. The main reason for this control is to protect children against explicit adult and inappropriate content. This article deals with Internet censorship in People's Republic of China.

2 Internet Censorship

Internet censorship and surveillance are very often interconnected in modern computer networks, such as the Internet. Many Internet Service Providers (ISP) are monitoring their users due to the accounting issues and spam protection. Once you are not using security tools for keeping your communication anonymous, it is very easy for your ISP to save and control the communication of its users. This is the basic prerequisite for technical censorship [1].

2.1 Censorship Methods

One of the basic methods of blocking the access to the information on the specific websites is based on the URL, IP address or specific keywords. Another way is to block access based on DNS (Domain Name System). Once the web browser sends a request for URL lookup for website that is blocked, DNS server sends a response with the incorrect or no information [2].

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 332–337, 2013.

Other methods include blocking according to the TCP/UDP port, traffic shaping rules in VoIP (Voice over IP) or Internet shutdown. This may occur in case of political events, such as revolutions.

2.2 Analysis Methods

Nowadays, analysis of Internet censorship is simple thanks to the projects that want to warn the rest of the world about the situation in the specific countries. The OpenNet Initiative is a project whose goal is to monitor and report on internet filtering and surveillance practices by nations. The reports are aimed for the public (more information is available on http://opennet.net/).

Another project is WatchMouse which provides simple service for testing the availability of a particular website. The services use the infrastructure of 62 stations in 26 countries (details can be found on http://www.watchmouse.com).

Chinese Firewall Checker is a product that enables users to find out if the given website is available in five different locations in China. List of most checked website is available as well. The Chinese Firewall Checker can be found on http://bestvpnservice.com/.

2.3 Circumvention Methods

There are several techniques how to circumvent Internet censorship. One of the most common way to access blocked content is to use HTTPS protocol or technologies as proxy servers, VPN (Virtual Private Network) and TOR (The Onion Router) [1].

Special versions of the websites might also lead to the desired content without being blocked. Modified websites for smartphones using URL starting with “m” or “mobile” can allow you to access the content that is not available on the parent website.

Another way to circumvent Internet censorship is to use services like Google Cache, RSS aggregators, website translators (Google Translate, Bing Translator, ...) or web archives (Wayback Engine).

3 Practical Results

In order to verify the Internet censorship in a certain country, first we have to have a direct access to the Internet from within that location. For the testing purposes in China, we have an access to the remote PC station physically located in Hangzhou. All results presented in this paper are based on tests performed from that PC station. Different results might be obtained from different locations in China.

3.1 DNS Cache Poisoning

First method of the Internet censorship identified in China is DNS cache poisoning. When trying to resolve the URL of a given website the obtained IP address differs

from the one obtained from locations outside of Mainland China. This might be an issue of a different server location, technique like anycast etc. The other explanation for this might be that the DNS response has been poisoned. It means that IP address does not belong to the website the user is trying to access. This is the case that happens in China. Let us look at the results of the dig command from Czech Republic.

```
$ dig www.youtube.com +short A
youtube-ui.l.google.com.
173.194.39.142
173.194.39.128
173.194.39.129
<output-omitted>
```

According to the output one of the IP addresses for YouTube is 173.194.39.142. The given IP address is owned by Google as we can see in the following output (lookup in the Whois database).

```
$ telnet whois.arin.net 43
Trying 199.71.0.47... Connected to whois.arin.net. Escape
character is '^]'.
173.194.39.142
<output-omitted>
OrgName: Google Inc. OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA PostalCode: 94043
Country: US
<output-omitted>
```

Now let's perform the same test from within the Mainland China. The results are different as we can see in the outputs below.

```
$ dig www.youtube.com +short A
59.24.3.173
$ telnet whois.apnic.net 43
Trying 202.12.29.220... Connected to whois.apnic.net. Es-
cape character is '^]'.
<output-omitted>
59.24.3.173
inetnum: 59.0.0.0 - 59.31.255.255 netname:KORNET
descr: KOREA TELECOM
descr: Network Management Center country: KR
<output-omitted>
```

Based on the results the resolved IP address is not only different but also owned by the organization outside the People's Republic of China. The result of such test is not always the same. Obtained IP addresses differ for a various websites. Results for a

certain websites differ over time as well. Websites where DNS cache poisoning was identified are Facebook, Twitter and YouTube. Table 1 contains IP addresses with their owners that were identified during the testing period. The previous results might seem a little bit confusing. Questions like "Why are poisoned IP addresses not registered by Chinese government?" or "Why are big telecommunication companies involved in Internet censorship?" can be answered with simple words "They might not know". When trying to connect to these IP addresses on HTTP port 80 the connection always fails on timeout. Deeper analysis of the IP addresses reveals that no port is open. Even ping fails with timeout. Simple conclusion is that the stations with the IP addresses are down or the IP addresses are not assigned to anybody. These IP addresses are within the registered range of a certain organizations but might not be used at all. The IP addresses might have been identified by Chinese government as those with no usage and were assigned just to simulate valid results. Visible output for a user when accessing blocked website is conclusive. The website is not available.

Table 1. Poisoned IP addresses and their owners

IP address	Location	Owner
8.7.198.45	USA	ARIN
37.61.54.158	Azerbaijan	Baktelekom
46.82.174.68	Germany	Deutsche Telecom
59.24.3.173	Korea	Korea Telecom
78.16.49.15	Ireland	Esat Telecommunications Limited
93.46.8.89	Italy	Fastweb
159.106.121.75	USA	DoD Network Information Center
203.98.7.65	New Zealand	Telstra Clear
243.185.187.39	USA	Internet Assigned Numbers Authority

Table 2. Examples of blocked keywords and expressions

Keyword Expression	Search engine		URL/keyword
	www.google.com	search.yahoo.com	en.wikipedia.org
Falun	Conn Reset	Conn Reset	Conn Reset
Peacehall	Conn Reset	Conn Reset	Conn Reset
Liu Xiaobo	Conn Reset	OK	Conn Reset
Great FW of China	Conn Reset	OK	OK
Free Tibet	OK	OK	Conn Reset

3.2 Connection Reset

Another way of the Internet censorship in China is a "Connection Reset by Peer" result when accessing the blocked website. The result is immediate and several reasons for this approach has been identified. First, the blocked keyword occurs in the URL. Second, the content of the website is not permitted within the Mainland China.

No keyword is always blocked. It always depends on the do- main. Some keywords are blocked as a content of a search parameters of search engines (Google, Yahoo, ...). Some keywords are blocked as a part of URL etc. Results of this kind of analysis should be interpreted very carefully because e.g. Google is quite often redirected to it's Hong Kong version which is much less restrictive. Table 2 contains several keywords with the associated censorship reaction.

According to the [3] the so-called "Great Firewall of China" operates, in part, by inspecting TCP packets for keywords that are to be blocked. If the keyword is present, TCP reset packets (with the RST flag set) are sent to both endpoints of the connection, which then close. However, because the original packets are passed through the firewall unscathed, if the endpoints completely ignore the firewall's resets, then the connection will proceed unhindered. Once one connection has been blocked, the firewall makes further easy-to-evade attempts to block further connections from the same machine. This latter behavior can be leveraged into a denial-of-service attack on third-party machines.

The way the TCP reset packets can be ignored includes `iptables` installed within Linux. With to following command:

```
iptables -A  INPUT  -p tcp --tcp-flags  RST RST -j DROP
```

which specifies that incoming TCP packets with the RST flag set are to be discarded. Once the TCP resets are discarded the website transfer will occur without any blocking [3].

4 Conclusion

Results presented in this paper were performed using remote PC station physically located in China. The station used is one particular PC located at one place (Hangzhou) therefore results are strongly dependent on that location. Results from other locations could be different.

Internet censorship in China is very widespread and used techniques falls into two categories: DNS cache poisoning and Connection Reset. There are several ways how to circumvent Internet censor- ship. One of them is to ignore RST packets. Other ways to circumvent censorship could be using technologies as proxy servers, VPN or TOR.

Future analysis of the Internet censorship could be based on the PC station where root account would be available. We could not perform deep tests of the censorship due to these limitations.

Acknowledgements. The research has been supported by Technology Agency of the Czech Republic (TACR) in frame of the project SCADA system for control and monitoring RT processes, TA01010632. This project has been also carried out with a financial support from the Czech Republic through the project no. MSM0021630528: Security-Oriented Research in Information Technology and by the project no. ED1.1.00/02.0070: The IT4Innovations Centre of Excellence; the part of the research has been also supported by the Brno University of Technology, Faculty of Information Technology through the specific research grants no. FIT-S-11-1 and by the project MPO CR, FR-TI1/037.

References

1. Deibert, R.J., Palfrey, J.G., Rohozinski, R., Zittrain, J.: Access Denied – ThePractice and Policy of Global Internet Filtering. The MIT Press (2008)
2. Stallings, W.: Cryptography and network security: principles and practice. Prentice Hall (1998)
3. Clayton, R., Murdoch, S.J., Watson, R.: Ignoring the Great Firewall of China. University of Cambridge, http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf