The Great Firewall of China

How It Blocks Tor and Why It Is Hard to Pinpoint

PHILIPP WINTER AND JEDIDIAH R. CRANDALL

Philipp Winter is a PhD student in the PriSec group at Karlstad University in Sweden. His work focuses on censorship resistance and analysis. Philipp would be happy if you would run a Tor relay if you are not operating one already.
philwint@kau.se

Jedidiah Crandall is an Assistant Professor at the University of New Mexico Department of Computer Science, where his research focuses on advanced inference techniques to understand the structure and operations of networks. He is also interested in natural language processing of Asian-language social media. He is typing this bio from behind the Great Firewall on a business trip, in Harbin where the dumplings and beer are excellent.
crandall@cs.unm.edu

Internet censorship is no longer a phenomenon limited to countries with a weak human rights record—the Western world is beginning to embrace the idea. This development leads to a fundamental research question: how can we know where the roadblocks are on the Internet and the details of how they work? In this article, we use the "Great Firewall of China" (GFC) to illustrate how complex of a problem it can be to find the network filtering devices, and how sophisticated the filtering itself can be when directed at an advanced target such as the Tor anonymity network.

The GFC is only a small part of the legal, regulatory, and technical mechanisms China has put in place for Internet censorship [6], but it is an important part because it helps to separate China's Internet from the Internet of the rest of the world. Without this, domestic control of Internet content would be moot because Chinese Internet users would simply seek out foreign Web sites where content was not controlled.

After all, the GFC is capable of much more than just filtering keywords. In this article, we will focus on two aspects.

We will first show the shortcomings in the current research literature that make it difficult to narrow down where Internet filtering occurs within China's Internet using Internet measurements.

In the second part of this article, we will show how the GFC is blocking the Tor anonymity network. Despite being originally designed as a low-latency anonymity network, Tor is increasingly used as a censorship circumvention tool.

Shortcomings in Our Understanding of China's Internet Censorship Implementation

What is censored is an important question to ask with respect to Internet censorship, but it is not directly related to the implementation of censorship and so will not be discussed in this section. There are two basic questions that should form the foundation for understanding any Internet censorship implementation in a given country: how is the filtering performed, and where does the filtering occur? In China, determining how filtering is performed is complicated because filtering implementations differ depending on location and, furthermore, can change over time. We discuss this issue in the following section and, with respect to the Tor network, later in this article. Where the filtering occurs is much more difficult to

determine in China because China's Internet has a unique topology and may tunnel a large amount of IPv4 traffic through IPv6 tunnels.

How Is the Filtering Performed in China?

In 2003 Zittrain and Edelman [9] performed perhaps the first academic work to collect data about what China was filtering and how that filtering was implemented. Much of the work that followed in 2006 and 2007 focused on the filtering of HTTP GET requests based on keywords [2]. The data showed that for GET requests containing sensitive keywords (e.g., "falun" in reference to the Falun Gong religion), routers in China in between the client and server would forge multiple TCP RST segments in both directions to try to reset the TCP connection. In Clayton et al. [2], sequence number matching was used to determine that this filtering was probably being performed by a bank of intrusion detection systems (IDSes), where the packets are allowed to pass through for performance reasons but port mirrored to the bank of IDSes, which could use RST injection to stop the flow of traffic for connections in which keywords appeared. The ConceptDoppler project [3] also did some packet-level measurements of keyword filtering for a wider array of routes approximately one year after Clayton et al. The difference in time and place for these two sets of measurements may account for several differences in the results.

For example, one question that is now resolved but illustrates the difficulties in answering basic questions about Internet censorship in China is whether GET request filtering is stateful. That is, does any GET request packet with a blacklisted keyword trigger TCP RST segments, or should the TCP handshake be completed and an actual connection established first? Previous work (e.g., [2, 3]) had drawn different conclusions, but more recent work [8] found that the filtering is now totally stateful. This discrepancy in the literature is probably because some routes were stateful and some were not, but over time all routes upgraded to have stateful filters. This heterogeneity in the implementation of filtering in China and the fact that it is always evolving create many challenges for measuring the censorship implementation.

GET request filtering is relatively easy to measure because it appears to be symmetric and bi-directional so that eliciting censorship is as simple as sending an offending GET request to any IP address in China. In fact, the reader can trigger filtering by simply opening the URL http://www.baidu.com/s?wd=falun. China implements other types of filtering, including DNS, Web content filtering, and application-level filtering on microblog servers. The type of filtering most relevant to how China blocks Tor, which would be filtering by IP address, has been less well studied in the past literature.

Where Does the Filtering Occur in China?

The question of where a particular type of filtering occurs can be posed in different ways, but typically we are interested in whether filtering occurs on specific routes but not on others, and possibly what router on that route is performing the filtering.

Again, GET request filtering has been the most studied implementation of censorship-related filtering in China in this respect because it is easy to solicit filtering from outside the country. Clayton et al. [2] observed that the time-to-live (TTL) field of forged TCP RST packets was larger than that of packets that really came

from the actual Web server on the other end of their connection. ConceptDoppler [3] manipulated the TTL field of packets with blacklisted keywords to locate which router on the route to each of the hosts within China they tested performed filtering and forged the RSTs. They concluded that the filtering was concentrated near the border but sometimes was as many as 13 hops beyond the border; 28% of the routes they tested had no filtering at all. Xu et al. [8] did a more comprehensive study and concluded that the filtering was occurring more at the provincial level.

In an article in the *Atlantic Monthly* in March 2008 [4], James Fallows wrote:

> In China, the Internet came with choke points built in. Even now, virtually all Internet contact between China and the rest of the world is routed through a very small number of fiber-optic cables that enter the country at one of three points: the Beijing-Qingdao-Tianjin area in the north, where cables come in from Japan; Shanghai on the central coast, where they also come from Japan; and Guangzhou in the south, where they come from Hong Kong. (A few places in China have Internet service via satellite, but that is both expensive and slow. Other lines run across Central Asia to Russia but carry little traffic.)

Xu et al.'s results and the fact that both GET request filtering and IP address filtering have at times been found not to occur on all routes into or out of China suggest a less centralized flow for China's international traffic. How does this square with Fallows' notion of a small number of choke points? The answer may lie in Internet Exchange Points (IXPs) and IPv4-over-IPv6 tunnels.

While the academic literature and online resources about IXPs seem only to refer to one IXP in Shanghai, the China Internet Network Information Center's (CNNIC) map of Internet connectivity in China (available at http://www1.cnnic.cn/images/info-stat/map1208.jpg) clearly shows three IXPs: in Beijing, Shanghai, and Guangzhou.

Why do these IXPs not appear in various efforts to locate IXPs on the Internet? The answer may lie in the fact that a large portion of China's Internet backbone appears to be implemented in IPv6, where IPv4 traffic is tunneled through in a "4-over-6" tunnel. "6-over-4" tunnels are more common and more well-studied than "4-over-6" tunnels, which along with IPv6 backbones create special challenges for any Internet measurement based on IPv4. Routing table information used in Internet topology measurements typically focuses on IPv4, and IPv4 traceroutes cannot detect hops inside an IPv6 tunnel because the TTL field will not be decremented in the IPv4 header. To measurements that are based on IPv4, "4-over-6" tunnels look like single hops. How much of China's Internet backbone is IPv6-based with IPv4 traffic being tunneled through? What percentage of international traffic traverses one of the three large IXPs in Beijing, Guangzhou, and Shanghai? The research literature does not have answers to these questions.

More Research Is Needed

Before we can begin to answer the question of where exactly Internet censorship filtering occurs within China's Internet, we need a better understanding of the structure of China's Internet. The roles of IPv6 and IXPs are key to this understanding. If a significant amount of China's backbone is IPv6, standard measurement techniques based on manipulating and observing IP TTLs will not allow us to find out which hop within this backbone is performing the filtering. It is possible that past efforts to locate the filtering, where the filtering has appeared to be near

the border [3] or at the local provincial level [8] may have simply been seeing either the entrance point or exit point of a "4-over-6" tunnel because the results were based on IPv4 TTLs. This is compounded by other problems with using TTLs, such as the fact that forged RSTs from China appear to now make attempts to choose TTLs that appear to be from the other end of the connection.

In summary, more research is needed into both the structure of China's Internet in general and how to locate filtering specifically.

IP address blacklisting may take place at the same routers that implement GET request filtering, or it may be an entirely different mechanism. In either case, the structure of China's Internet will play a key role in the percentage of routes into or out of China that successfully block blacklisted IP addresses. Furthermore, it is likely that IP address blacklisting in China, like other mechanisms, is heterogeneous in the sense that various ISPs and different parts of the network may implement it differently (e.g., null routing, forged RSTs, network address translation, etc.).

The GFC and Tor

With roughly 400,000 daily users and 3,000 relays, Tor is the most popular low-latency anonymity network. Despite being originally designed for anonymity only, Tor turned out to be a good tool to circumvent censorship equipment and is now increasingly used for this purpose. This trend did not remain unnoticed by censors and is the reason why Tor is receiving special attention by the GFC, among others.

The Past

For several years, the Tor network has been in a cat-and-mouse game with the GFC. The first documented attempt to block Tor happened back in 2008. Users behind the GFC in China noticed that the official Tor Web site, www.torproject.org, stopped being reachable. As it turned out, deep packet inspection (DPI) boxes were scanning network traffic for the substring `torproject.org` in HTTP requests. When this substring was found, spoofed TCP reset segments were sent to both endpoints. Four years later (2012), this is still the case but can be circumvented easily by using HTTPS instead of plain HTTP. The DPI boxes are not able to detect the substring if the traffic is encrypted.

Although this type of block simply prevented users from downloading the Tor Browser Bundle from the official Web site (note that there are plenty of mirrors operated by volunteers), a user who somehow got her hands on a copy of the Tor client could still use the network without interference.

One year later, in 2009, the GFC's functionality was extended also to block all public relays as well as the directory authorities by simple IP blocks. The directory authorities serve the consensus, which is a directory containing all public Tor relays. The directory is downloaded by Tor clients during the bootstrapping phase, and blocking this step effectively blocked the public Tor network. But, at this point, the Tor developers had already implemented the concept of bridges, which are unpublished relays. Bridges are meant to provide a semi-hidden stepping-stone for censored users into the network. Along with bridges comes the bridge distribution problem: while in an ideal world, bridges should only be given to censored users, a censor can always mimic users and obtain—and then block—bridge addresses the same way. The current approach to the bridge distribution problem is to make it

easy to get some of them but hard to get all of them, because then a censor could simply block them all. While the public network was blocked at this point in China, bridges remained functioning and were used heavily.

The increasing popularity of bridges did not remain unnoticed, though. Several months later, in March 2010, the Chinese bridge usage statistics started to drop significantly as shown on the right end in Figure 1. An explanation for this sudden drop was provided in a blog post: The GFC started to block some of the more popular bridges.

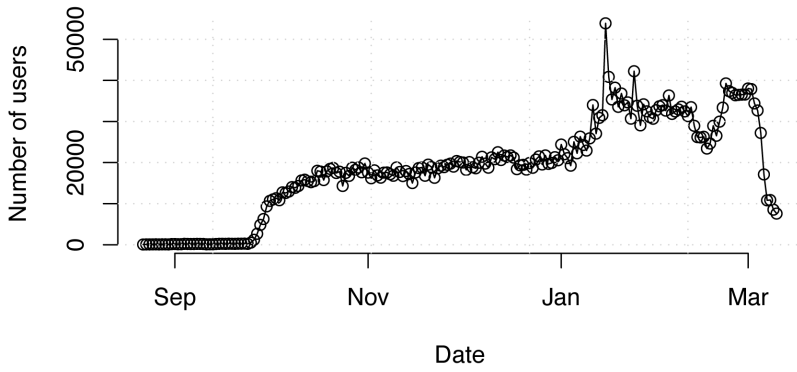

Figure 1: Bridge users connecting from China between 2009 and 2010

Bridges can be configured to be either public or private. A public bridge announces its existence to the public bridge database operated by the Tor developers so that it can be distributed automatically to people who need a bridge. A private bridge remains silent and hence only known to its operator.

At this point in the arms race it was still possible to set up private bridges and manually give their addresses to trusted people in China. For many months, private bridges remained a working, if less-than-ideal, solution to the unreachable public Tor network as well as to the mostly blocked public bridges; however, this changed in late 2011, when the GFC made the next move in the arms race. While the GFC's above-mentioned blocking attempts consisted mostly of simple IP blocks and Web site crawling, the next section outlines a drastic increase in sophistication and complexity.

The Present

In October 2011 a user reported on the Tor bug tracker that even private bridges appeared to get blocked within only minutes of their first use. As illustrated in Figure 2, the GFC is now using a novel two phase approach to make this possible [7]. In the first phase, Chinese egress traffic is being scanned for what appears to be Tor connections and the second phase is meant to confirm this suspicion by reconnecting to the suspected bridges and trying to initiate a Tor connection. The following two sections will present these two phases in greater detail.

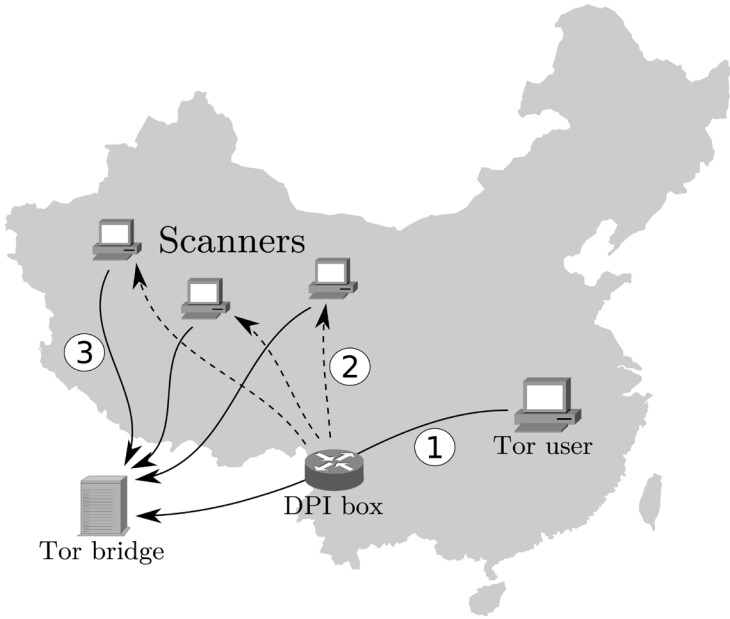

Figure 2: The GFC is (1) identifying Tor connections and (2) preparing scanners, which then (3) conduct follow-up scanning to verify that a Tor bridge was used

PHASE 1: FINGERPRINTING OF TOR

The GFC fingerprints Tor connections by exploiting the fact that Tor's TLS handshake slightly stands out from other applications' use of TLS. In particular, Chinese DPI boxes are looking for the cipher list, which is part of the TLS client hello. The cipher list is used by the Tor client to tell the bridge which cryptographic ciphers it supports. In particular, Tor's cipher list (for versions older than 0.2.3.17-beta) is a static string of 58 bytes. The following 58 bytes are what the DPI boxes are looking for in egress traffic:

```
0ac0 14c0 3900 3800 0fc0 05c0 3500 07c0 09c0 11c0
13c0 3300 3200 0cc0 0ec0 02c0 04c0 0400 0500 2f00
08c0 12c0 1600 1300 0dc0 03c0 fffe 0a00 ff00
```

For a long time, this cipher list was identical to the one used by Firefox 3. The Tor developers mimicked Firefox's cipher list in an attempt to make the Tor TLS handshake look like a Firefox connecting to an Apache Web server; however, newer versions of OpenSSL started adding `TLS_EMPTY_RENEGOTIATION_INFO_SCSV` to the cipher list, which made Tor's TLS handshake look different from Firefox 3 again.

PHASE 2: FOLLOW-UP SCANNING

Once Chinese DPI boxes discover a Tor-specific cipher list on the wire, follow-up scanning is initiated. Several minutes after the Tor handshake, two to three random Chinese IP addresses reconnect to the bridge just used by a Chinese user. These scanners connect to the bridge, start a TLS session, and then try to create a Tor circuit. If this succeeds, the bridge finds itself on the blacklist shortly thereafter. This blacklist consists of IP:Port tuples. Bridges and relays are not simply blacklisted by IP address. This might lead to overblocking, i.e., blocking

more than actually necessary. Perhaps in an attempt to avoid this problem and minimize collateral damage, the GFC operators chose to block bridges by IP address and port. The blacklist probably holds around 4,000 such tuples (roughly 3,000 relays and 1,000 bridges).

The obvious step at this point would be for bridges to simply block these scanners. Unfortunately, the scanners mimic real computers very well. They come from almost random Chinese IP addresses, and the few properties in which they differ from real computers are hard to exploit effectively.

Evasion

Before discussing how the Tor network can be made more resistant to blocking attempts, we first describe the two fundamental ways in which Tor—and any other censorship evasion system—can be blocked:

BLOCK-BY-PROTOCOL

DPI boxes can be looking for Tor-specific signatures in the traffic exchanged by client and server. Ethiopia, for example, is blocking Tor by matching for signatures in the TLS client hello and server hello. If such a signature is found, the respective packet is simply dropped.

BLOCK-BY-ENDPOINT

Alternatively, Tor can be blocked by simply harvesting all relays and as many bridges as possible and blacklisting the respective IP addresses. Unfortunately, this is still a viable strategy.

EVADING PROTOCOL FILTERING

Protocol filtering can be evaded by obfuscating, scrambling, and reshaping a given network protocol to a degree that it is hard for DPI boxes to identify the target protocol. This can be done by simply exploiting "features" in TCP and IP or by adding a thin obfuscation layer between the transport and the application protocol. Both approaches can make the job of DPI boxes significantly harder.

The former is implemented by software such as fragroute (see http://www.monkey.org/~dugsong/fragroute/) or SniffJoke (see https://github.com/vecna/sniffjoke). Both projects exploit the fact that there is not enough information on the wire for a DPI box to fully reconstruct what is happening between two endpoints.

The latter is realized by a tool called obfsproxy, which is a network proxy developed by the Tor project. It is run as a local SOCKS proxy on the client-side as well as on the server-side. The actual obfuscation is handled by so-called pluggable transport modules. As long as the same module is loaded on both sides, the network traffic is being scrambled as dictated by the respective modules.

At this point, the only publicly available module for obfsproxy is called obfs2, which scrambles the network traffic so that no static fields remain that would be good candidates for fingerprinting. After a minimal handshake, the two parties have one symmetric session key each, which is used to build another layer of encryption over Tor's TLS connection.

EVADING ENDPOINT FILTERING

Assuming a perfect world in which Tor's transport protocol is unblockable, censors could still harvest and block the IP addresses of all bridges. After all, bridges are supposed to end up in the hands of legitimate users who need them, but not in the hands of evil censors; however, censors can always act as legitimate users to harvest addresses.

As already discussed above, the pragmatic approach so far has been to make it easy for a user to obtain a few bridges but hard to get many. Unfortunately, this approach is not very future-proof. Nation-state adversaries have lots of human resources, computational power, money, bandwidth, and IP address pools. Coming up with bridge distribution strategies that are robust against this kind of adversary is increasingly difficult.

Still, there is a glimpse of hope on the horizon. The recently proposed flash proxies concept by Fifield et al. [5] turns Web site visitors outside the censoring regime into short-lived stepping stones into the Tor network. The short-livedness is an advantage as well as a disadvantage. The disadvantage is that long-lived TCP connections can get terminated frequently. The advantage is that the mere volume of Web site visitors can be too much for a blacklist to handle. The censor should get overwhelmed by the sheer number of endpoints to block and discontinue blacklisting.

Conclusion

In this article, we gave an overview of the difficulties in determining in detail where filtering is taking place and how it is done. We used the Great Firewall of China and its ability to block the Tor anonymity network as an example.

Internet censorship is a relatively young field of research. Much more work needs to be done—both, in the field of measurement and circumvention—to keep the Internet free and information flowing freely. Current censorship research is exploring different areas. Blocking-resistant transport protocols that are being proposed appear to be pure randomness or mimic other protocols such as Skype or HTTP. Other research proposes to move circumvention to the Internet backbone or use Web site visitors as short-lived proxies. All in all, Internet censorship promises to be an exciting field of research with many important, challenging problems that will require bright minds to solve them.

References

[1] For a complete list of references, see: https://www.usenix.org/login-1212-winter-references.

[2] R. Clayton, S.J. Murdoch, and R.N.M. Watson, "Ignoring the Great Firewall of China," *I/S: A Journal of Law and Policy for the Information Society,* vol. 3, no. 2 (2007), pp. 70–77.

[3] J.R. Crandall, D. Zinn, M. Byrd, E. Barr, and R. East, "ConceptDoppler: A Weather Tracker for Internet Censorship," *Proceedings of the 14th ACM Conference on Computer and Communications Security* (ACM, 2007), pp. 352–365.

[4] J. Fallows, "The Connection Has Been Reset," *Atlantic Monthly,* March 2008: http://www.theatlantic.com/magazine/archive/2008/03/-the-connection-has-been-reset/306650/, accessed Sept. 6, 2012.

[5] D. Fifield, N. Hardison, J. Ellithorpe, E. Stark, R. Dingledine, P. Porras, and D. Boneh, "Evading Censorship with Browser-Based Proxies," *Proceedings of the 12th Privacy Enhancing Technologies Symposium* (Springer, 2012), pp. 239–258.

[6] The Open Net Initiative, China: http://opennet.net/research/profiles/china, accessed Sept. 6, 2012.

[7] P. Winter and S. Lindskog, "How the Great Firewall of China Is Blocking Tor," *Proceedings of the 2nd Workshop on Free and Open Communications on the Internet* (Bellevue, WA, USA, 2012), USENIX Association.

[8] X. Xu, Z.M. Mao, and J.A. Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Proceedings of the 12th International Conference on Passive and Active Measurement* (Springer, 2011), pp. 133–142.

[9] J. Zittrain and B. Edelman, "Internet Filtering in China," *IEEE Internet Computing,* vol. 7, no. 2, 2003, pp. 70–77.

Statement of Ownership, Management, and Circulation, 10/1/12

Title: ;login: Pub. No. 0008-334. Frequency: Bimonthly. Number of issues published annually: 6. Subscription price $125.

Office of publication: USENIX Association, 2560 Ninth Street, Suite 215, Berkeley, CA 94710.

Headquarters of General Business Office of Publisher: Same. Publisher: Same.

Editor: Rik Farrow; Managing Editor: Rikki Endsley, located at office of publication.

Owner: USENIX Association. Mailing address: As above.

Known bondholders, mortgagees, and other security holders owning or holding 1 percent or more of total amount of bonds, mortgages, or other securities: None.

The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes have not changed during the preceding 12 months.

Extent and nature of circulation	*Average no. copies each issue issue during preceding 12 months*	*No. copies of single issue (Oct. 2012) published nearest to filing date*
A. Total number of copies	4063	3850
B. Paid circulation		
Outside-county mail subscriptions	2229	1858
In-county subscriptions	0	0
Other non-USPS paid distribution	1206	1051
Other classes	0	0
C. Total paid distribution	3435	2909
D. Free distribution by mail		
Outside-county	0	0
In-county	0	0
Other classes mailed through the USPS	66	51
E. Free distribution outside the mail	472	660
F. Total free distribution	538	711
G. Total distribution	3973	3620
H. Copies not distributed	90	230
I. Total	4063	3850
Percent Paid and/or Requested Circulation	86%	75%
Paid Electronic Copies	272	273
Total Paid Print Copies + Paid Electronic Copies	3707	3182
Total Print Distribution + Paid Electronic Copies	4245	3893
Percent Paid (Both Print and Electronic Copies)	87%	81%

I certify that the statements made by me above are correct and complete.
Casey Henderson, Co-Executive Director 10/1/12