Scary: A really scary Pluggable Transport

My subtitle*

Carolin Zöbelein†
Independent mathematical scientist
Josephsplatz 8, 90403 Nürnberg, Germany

ABSTRACT

STATUS: Draft

KEYWORDS

Tor, Bridge, Scary, Obscuration, Censorship, Circumvention, Pluggable Transport

PREAMBLE

This paper was written in the context of a job application as Pluggable Transport Software Developer for Anti-Censorship Team of The Tor Project[1].

1 INTRODUCTION

In August 2018, The Intercept published a story about plans of Google for launching a censored version of its search engine in China, which will blacklist websites and search terms about human rights, democracy, religion, and peaceful protest [3]. This project, with the code-name *Dragonfly*, started in spring prior year, is the newest step in the ongoing work of creating a censored environment of information in China.

If we look back, the story of censorship in China started in 1998. The Communist Party feared that the China Democracy Party would create a powerful new network. The China Democracy Party was immediately banned, members arrested and imprisonment [2]. Finally, this resulted in the beginning of the *Great Firewall (GFW)* project, a combination of legislative actions and technologies enforced by the People's Republic of China to regulate the Internet domestically. It blocks access to selected websites, internet tools, mobile apps and slows down cross-border internet traffic.

Since the GFW blocks destinations and inspects the data being transmitted, ways for censorship circumvention need proxy nodes and encrypted data traffic. Typically, this is done these days by the help of foreign proxy servers, regional website mirrors, Tor, virtual private networks (VPNs) and secure shell (SSH).

Over the years, more and more of this circumvention tools have been blocked due to deep packet inspections and the detailed analysis of its content. So now, many VPNs are no longer useable to circumvent the Great Firewall of China and also the access to the Tor anonymity network [4], with its public list of relays, is no longer possible.

To solve the problem of relay blocking, Tor introduced so-called *bridges* [6] which are non-public relays, to help censored users reach the Tor network. Because of the ability of dynamically blocking bridges by looking for their TLS fingerprint [8] [1], packet fragmentation and Tor obfsproxy in combination with private bridges, were added [8].

Finally, this lead us to *Pluggable Transports (PT)* [7], which help to bypass censorship attempts against Tor. PTs transform the Tor traffic between client and bridges, in such a way that it looks like innocent traffic instead of the actual Tor traffic. In this paper, we will talk about this PTs, their general construction constraints and an introducing of an sketch of a new PT called *Scary*.

1.1 Outline

1.2 Notation

2 TLS FINGERPRINTING

3 CONCLUSIONS

A APPENDIX

A.1 Definitions

- **Virtual private network (VPN).** TODO
- **Secure shell (SSH).** TODO
- **Bridges.** TODO
- **Pluggable Transport (PT).** TODO

REFERENCES

[1] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. 2015. Analyzing the Great Firewall of China Over Space and Time. *PoPETs* 2015 (2015), 61–76.
[2] https://en.wikipedia.org/wiki/Great_Firewall. 2018. Great Firewall. (2018).
[3] https://theintercept.com/2018/08/01/google-china-search-engine-censorship/. 2018. Google plans to launch censored search engine in China, Leaked documents reveal. (2018).
[4] https://www.torproject.org/. 2018. The Tor Project. (2018).
[5] https://www.torproject.org/about/jobs-developer-anti-censorship.html.en. 2018. Internet Freedom Nonprofit Seeks Software Developer for Anti-Censorship Team. (2018).
[6] https://www.torproject.org/docs/bridges.html.en. 2018. Tor: Bridges. (2018).
[7] https://www.torproject.org/docs/pluggable-transports.html.en. 2018. Tor: Pluggable Transports. (2018).
[8] Philipp Winter and Stefan Lindskog. 2012. How the Great Firewall of China is blocking Tor. In *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI 2012)*.

LICENSE

*The author believes in the importance of the independence of research and is funded by the public community. If you also believe in this values, you can find ways for supporting the author's work here: https://research.carolin-zoebelein.de/crowdfunding.html

†https://research.carolin-zoebelein.de, *E-mail address:* contact@carolin-zoebelein.de, PGP: D4A7 35E8 D47F 801F 2CF6 2BA7 927A FD3C DE47 E13B

[1]The Tor Project, Inc., is a 501(c)(3) nonprofit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies. [5]

September 28, 2018.