Obfs2

Pluggable Transports documentation series.*

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 is part of a paper documentation series about Pluggable Transports (PTs) [3], how they work and their strengths and weaknesses.

1 INTRODUCTION

During the history of digital networks, we have been confronted more and more with the phenomenon of internet censorship and blocking by governments [4]. So, over the years, more and more circumvention tools were developed and also have been blocked due to deep packet inspections and the detailed analysis of its content. This lead us to, so-called, *Pluggable Transports (PTs)* [3], which help to bypass censorship attemps by transforming the traffic between client and server, in such a ways that it looks like innocent traffic.

In this paper, we will talk about *obfs2*, a protocol obfuscation layer for TCP protocols. We will show how it works, what we can do with it and which strengths and weaknesses it has.

1.1 Outline

TODO

1.2 Notation

TODO

2 OBFS2

Obfs2 is a protocol obfuscation layer for TCP protocols, to keep a third party from telling what protocol is in use based on message contents [2]. It's the continuation of brl's ssh obfuscation protocol [2] [1].

3 CONCLUSIONS

A APPENDIX

REFERENCES

[1] https://github.com/brl/obfuscated-openssh. 2009. GitHub: Handshake Obfuscation. (2009).
[2] https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/tree/doc/obfs2/obfs2-protocol-spec.txt. 2015. Obfs2 specification. (2015).
[3] https://www.torproject.org/docs/pluggable-transports.html.en. 2018. Tor: Pluggable Transports. (2018).
[4] 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

October 27, 2018.