Workgroup: Network Working Group
Internet-Draft:
draft-cfm-circumvention-cap-theorem-01
Published: 26 November 2023
Intended Status: Informational
Expires: 29 May 2024
Authors: C. Myers
ARTICLE 19

Towards a CAP Theorem for Censorship Circumvention

Abstract

This Internet-Draft is a submission to the IAB Workshop on Barriers to Internet Access of Services [biasws].

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-cfm-circumvention-cap-theorem/.

Source for this draft and an issue tracker can be found at https://github.com/cfm/draft-cfm-circumvention-cap-theorem.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 May 2024.

(https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Research proposal
2. Informative References

Author's Address

1. Research proposal

Between June 2022 and April 2023 [tor-status], the Tor network was the target of a sustained distributed denial-of-service (DDoS) attack, apparently targeting the relays and directory servers that coordinate introductions to Tor hidden services [tor-relays-2022-07] [tor-relays-2022-10]. This attack impeded the performance and threatened the security of the Tor network for all users. It especially obstructed Web sites and services that had gone out of their way to be accessible to Tor users via Tor hidden services, which usually improve the performance of the Tor network by bypassing the "exit nodes" that interface with the clearnet Internet.

Although the origins and motivations of this attack remain unknown, it is a useful case study in the D/DoS vulnerability of overlay networks such as Tor, which users may seek out to protect their anonymity, circumvent censorship, or both. The CAP theorem [cap-theorem] is instructive: like a database, a censorship-circumvention system is useful to the extent that it is:

1. **consistent:** returns accurate and current data;

2. **available:** returns data at all; and

3. **partition-tolerant**: routes around failures, which by definition include active censorship. In this case, they also include active *attacks* on circumvention infrastructure that lessen its overall availability, whether or not intended as an act of censorship.

For the workshop, I propose to explore further whether formalisms such as the CAP theorem are useful models and/or measures for the utility and resilience of a censorship-circumvention system such as Tor.

2. Informative References

[biasws]

Internet Architecture Board, "Workshop on Barriers to Internet Access of Services", 20 September 2023, <https://datatracker.ietf.org/group/biasws/about/>.

[cap-theorem] "CAP theorem", n.d., <https://en.wikipedia.org/wiki/CAP_theorem>.

[tor-relays-2022-07] Dingledine, R., "We're trying out guard-n-primary-guards-to-use=2", 6 July 2022, <https://lists.torproject.org/pipermail/tor-relays/2022-July/020686.html>.

[tor-relays-2022-10] Koppen, G., "DoS attacks -- status update", 28 October 2022, <https://lists.torproject.org/pipermail/tor-relays/2022-October/020858.html>.

[tor-status] Tor Project, "Network DDoS", 9 June 2022, <https://status.torproject.org/issues/2022-06-09-network-ddos/>.

Author's Address

Cory Myers
ARTICLE 19

Email: cfm@acm.org