Timeless Timing Attacks and Preload Defenses in Tor’s DNS Cache
August 10, 2023
Rasmus Dahlberg and Tobias Pulls
first.last@kau.se
Overview

Users → Guard → Middle → Exit → Websites

Contains a DNS cache

Reliable probing attack
“Is example.com in the cache?”

Redesign Tor’s DNS cache
No dynamic cross-circuit sharing

Mitigation
Course-grained timing

https://gitlab.torproject.org/rgdd/ttapd
Outline

Included: how our attack and defense works, some key measurement results

Excluded: mitigation, more DNS exit measurements, traffic analysis applications

---

1 Pulls and Dahlberg: Website Fingerprinting with Website Oracles. In: PETS (2020)

https://gitlab.torproject.org/rgdd/ttapd
What you need to know about Tor’s DNS cache

Single-threaded Tor process
Make two requests arrive together, observe the order of responses\(^2\)

Attack accuracy in the live Tor network?

100%³

³Low cost, can run on a laptop with spotty WiFi
A false positive defense from Tor’s perspective

1. rm -rf /path/to/tor/dns/cache
   ▶ Exit configuration: ISP resolver
2. Add a per-circuit cache, no sharing
3. Add a static preload cache, shared

---

Exit measurements in the live Tor network

- Tor research safety board request
- Two exits during May-Sep, 2023
- Baseline performance? 11-17%
- Preload performance, what lists?
- Lists need no frequent updates

https://gitlab.torproject.org/rgdd/ttapd
Conclusions

- Is example.com in a relay’s DNS cache? 100%
- Narrows down the destination anonymity set
- Preloaded DNS cache
  - Yay: efficient and effective, “false positives”
  - Doh: we need a popularity list to preload
  - Doh: stay away from self-hosted resolver

Do you have a better defense idea? Get involved!

https://www.teepublic.com/t-shirt/
1674643-the-floor-is-dns
Bonus: timeline and useful links

- Informal chats with TPO, Refine idea
- Sloppy PoC
- Formal bug report
- Address safety board comments
- Live preload measurements
- Mitigation deployed
- Embargo lifted

- Jul 2020
- Aug 2020
- Dec 2020
- Dec 2021
- May 2022
- Sep 2022
- Dec 2022
- Mar 2023

---

1 Pulls and Dahlberg: Website Fingerprinting with Website Oracles. In: PETS (2020)
3 https://gitlab.torproject.org/tpo/core/tor/-/issues/40674