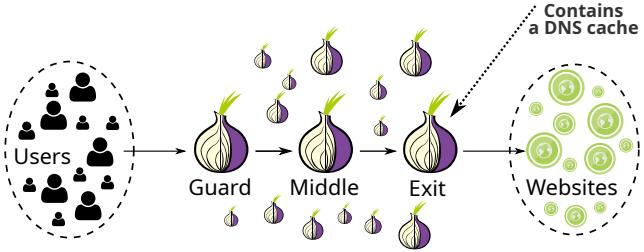
Timeless Timing Attacks and Preload Defenses in Tor's DNS Cache

August 10, 2023

Rasmus Dahlberg and Tobias Pulls

first.last@kau.se

Overview



Reliable probing attack
"Is `example.com` in the cache?"

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

Mitigation
Course-grained timing

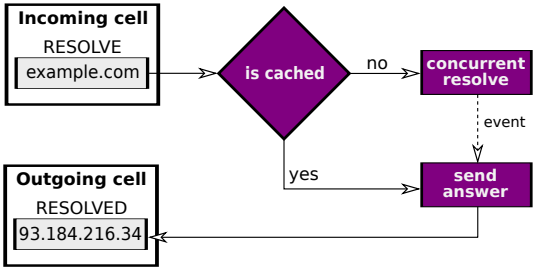
Outline

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

Excluded: mitigation, more DNS exit measurements, traffic analysis applications[1]

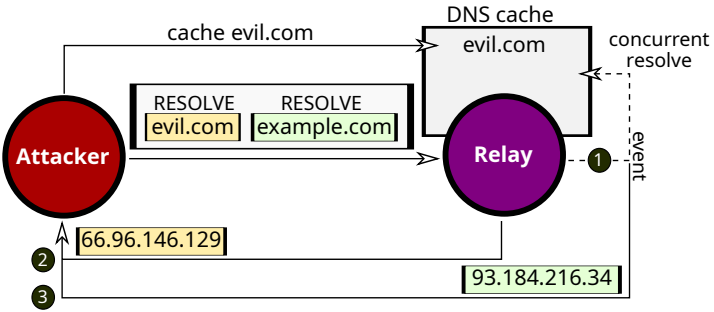
[1] Pulls and Dahlberg: Website Fingerprinting with Website Oracles. In: PETS (2020)

What you need to know about Tor's DNS cache



Single-threaded Tor process

Attack outline



Make two requests arrive together, observe the order of responses[2]

[2] Van Goethem *et al.*: Timeless Timing Attacks: Exploiting Concurrency to Leak Secrets over Remote Connections. In: USENIX Security (2020)

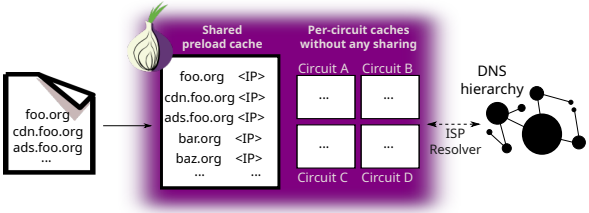
Attack accuracy in the live Tor network?

100%[3]

[3] Low cost, can run on a laptop with spotty WiFi

A false positive defense from Tor's perspective

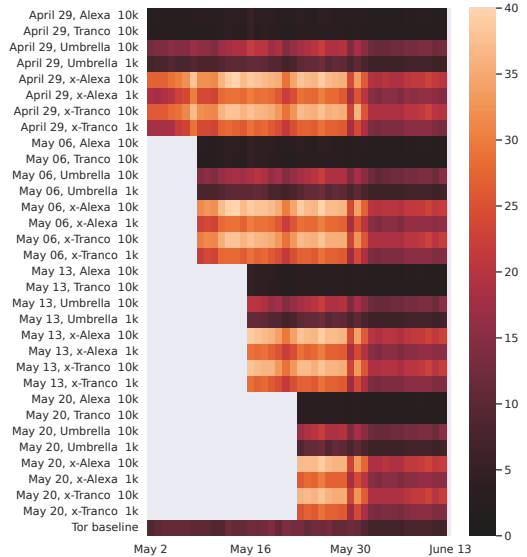
1. `rm -rf /path/to/tor/dns/cache`
   - Exit configuration: ISP resolver[4]
2. Add a **per-circuit cache**, no sharing
3. Add a static **preload cache**, shared



[4] Greschbach *et al.*: The effect of DNS on Tor's anonymity. In: NDSS (2017)

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



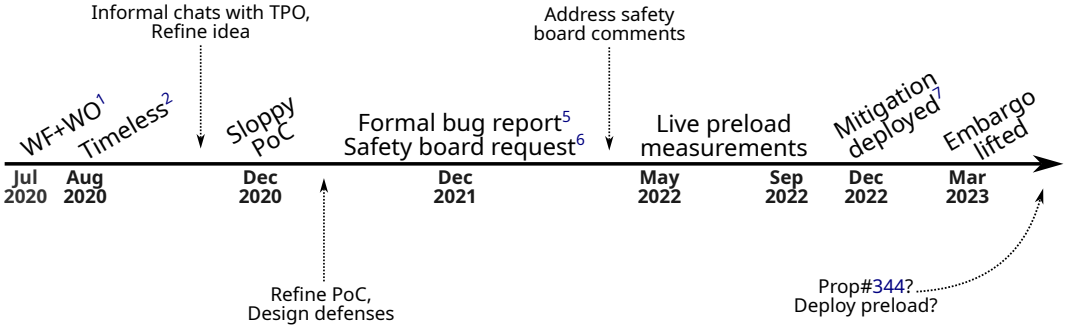
Conclusions

- 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

https://www.teepublic.com/t-shirt/1674643-the-floor-is-dns

Do you have a better defense idea? Get involved!

Bonus: timeline and useful links



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

[2] Van Goethem *et al.*: Timeless Timing Attacks: Exploiting Concurrency to Leak Secrets over Remote Connections. In: USENIX Security (2020)

[5] https://gitlab.torproject.org/tpo/core/tor/-/issues/40674

[6] https://gitlab.torproject.org/rgdd/ttapd/-/blob/main/artifact/safety-board/README.md

[7] https://gitlab.torproject.org/tpo/core/tor/-/blob/main/ReleaseNotes#L148-150