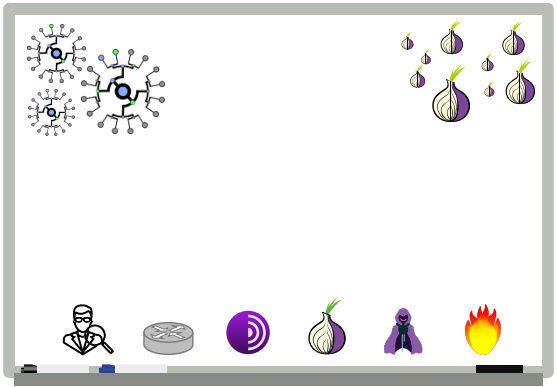
On Certificate Transparency Verification and Unlinkability of Websites Visited by Tor users

June 12, 2023

Rasmus Dahlberg

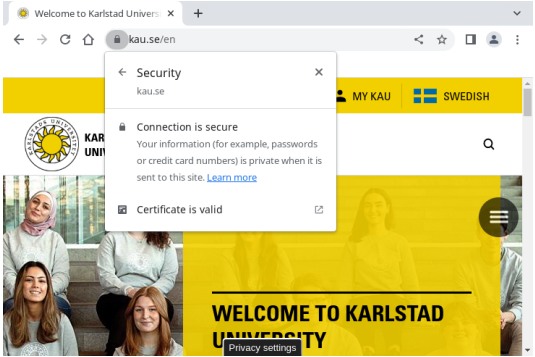
rasmus.dahlberg@kau.se

Outline

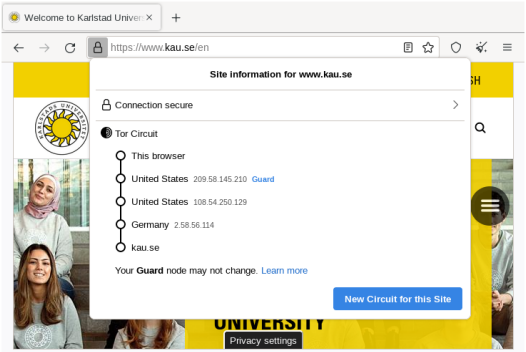


1. Introduction
2. Thesis overview
3. Contributions
4. Take away

How is all of this related to you?

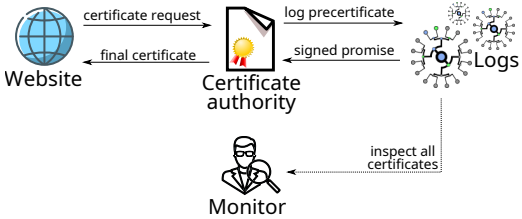


Web browsing

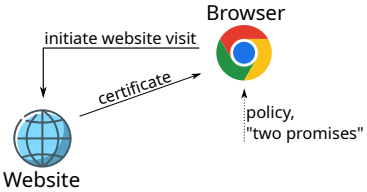


Possibly with Tor Browser

Some preliminaries, Certificate Transparency what?

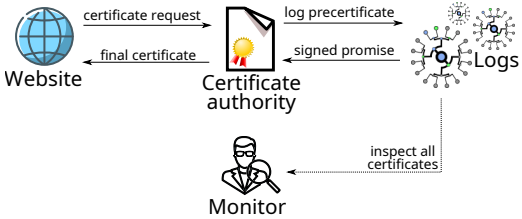


Certificate issuance

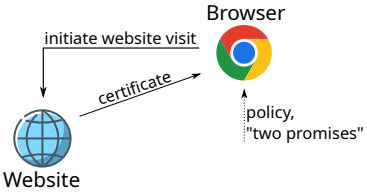


Browser behavior

Some preliminaries, Certificate Transparency what?



Certificate issuance



Browser behavior

Why should we take log promises at face value?

Research questions

1. Can trust requirements in Certificate Transparency be reduced in practise?

Research questions

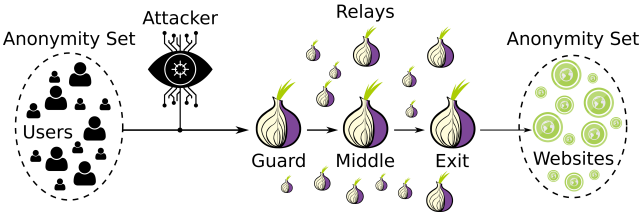
1. Can trust requirements in Certificate Transparency be reduced in practise?
2. How can authentication of websites be improved in the context of Tor Browser?

Research questions

1. Can trust requirements in Certificate Transparency be reduced in practise?
2. How can authentication of websites be improved in the context of Tor Browser?
3. How do the protocols used during website visits affect unlinkability between Tor users and their destination websites?

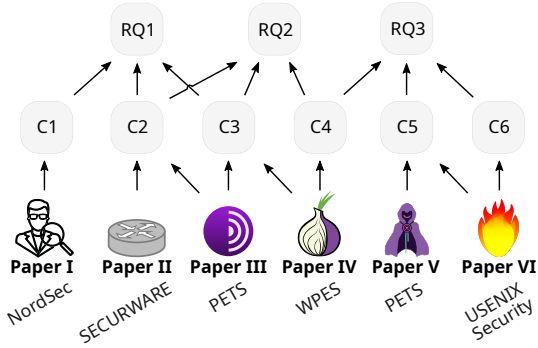
Research questions

1. Can trust requirements in Certificate Transparency be reduced in practise?
2. How can authentication of websites be improved in the context of Tor Browser?
3. How do the protocols used during website visits affect unlinkability between Tor users and their destination websites?



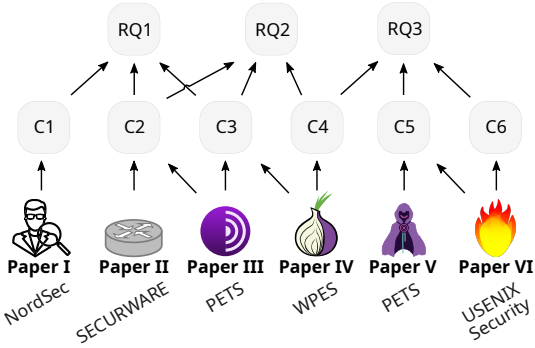
RQ1: "less trust reqs in CT" **RQ2:** "CT+Tor" **RQ3:** "exploit protocols for deanonymization"

Contributions



Contributions

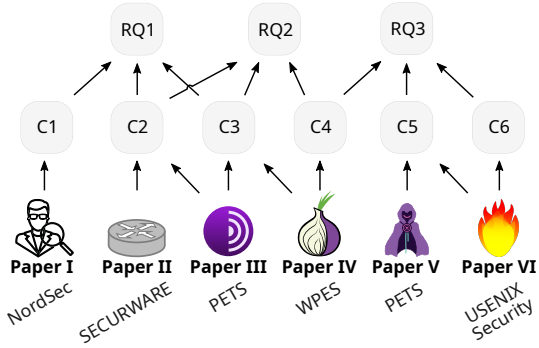
1. Reduced trust in third-party monitoring



RQ1: "less trust reqs in CT" **RQ2:** "CT+Tor" **RQ3:** "exploit protocols for deanonymization"

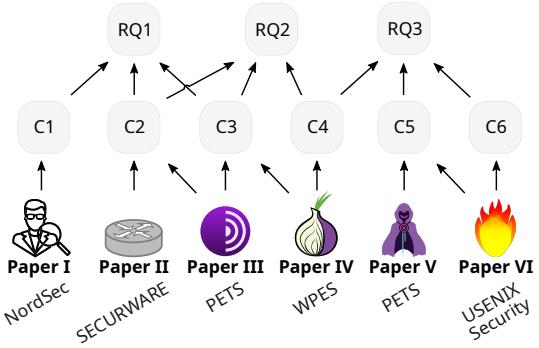
Contributions

1. Reduced trust in third-party monitoring
2. Increased probability of split-view detection



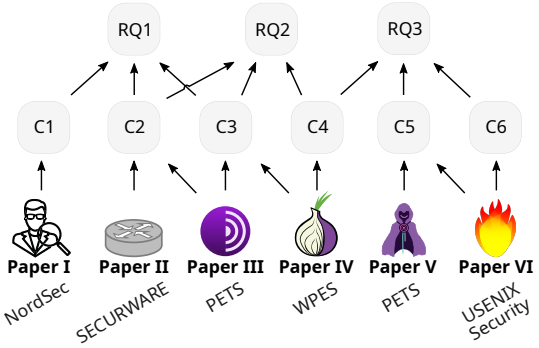
Contributions

1. Reduced trust in third-party monitoring
2. Increased probability of split-view detection
3. Improved detectability of website hijacks targeting Tor Browser



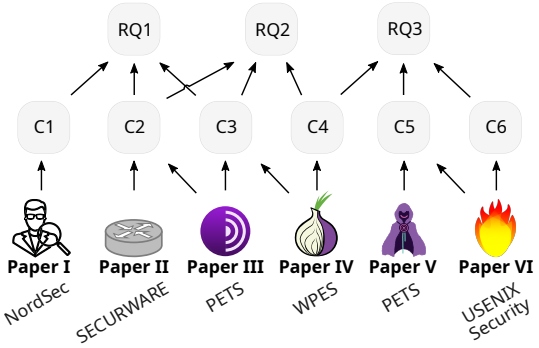
Contributions

1. Reduced trust in third-party monitoring
2. Increased probability of split-view detection
3. Improved detectability of website hijacks targeting Tor Browser
4. An extension of the attacker model for website fingerprinting



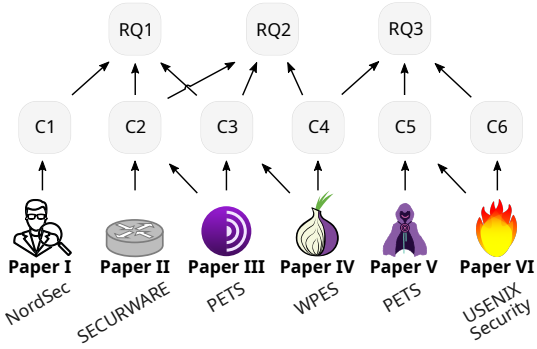
Contributions

1. Reduced trust in third-party monitoring
2. Increased probability of split-view detection
3. Improved detectability of website hijacks targeting Tor Browser
4. An extension of the attacker model for website fingerprinting
5. Remotely-exploitable probing-attacks on Tor's DNS cache

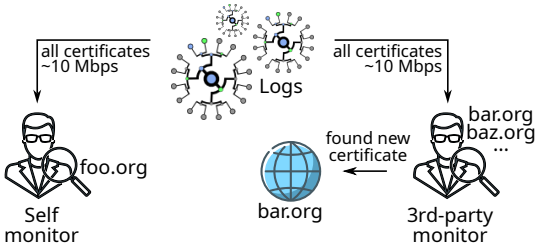


Contributions

1. Reduced trust in third-party monitoring
2. Increased probability of split-view detection
3. Improved detectability of website hijacks targeting Tor Browser
4. An extension of the attacker model for website fingerprinting
5. Remotely-exploitable probing-attacks on Tor's DNS cache
6. A redesign of Tor's DNS cache to defend against all (timeless) timing attacks

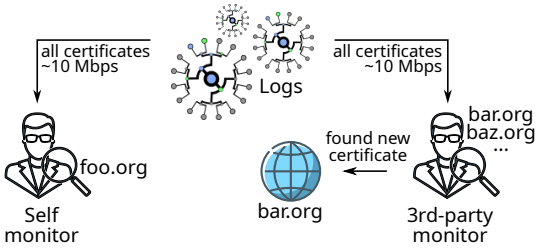


C1: Reduced trust in third-party monitoring

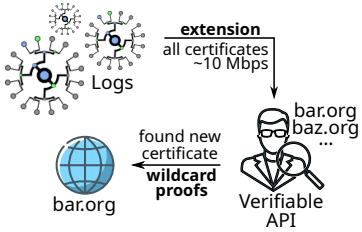


Problem

C1: Reduced trust in third-party monitoring

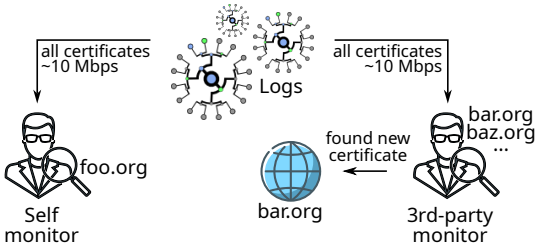


Problem

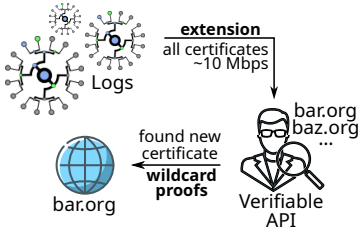


Solution

C1: Reduced trust in third-party monitoring



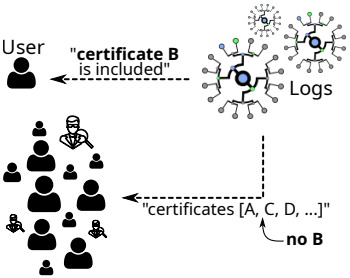
Problem



Solution

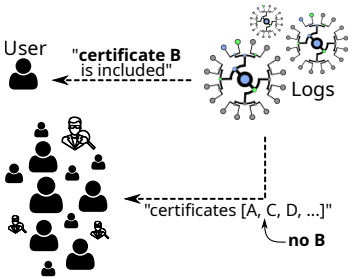
Secure in multi-instance setting, small performance overhead

C2: Increased probability of split-view detection

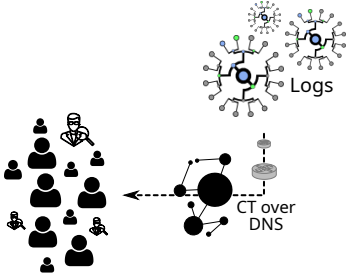


Problem

C2: Increased probability of split-view detection

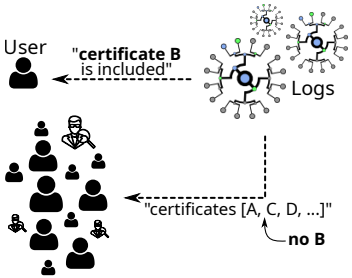


Problem

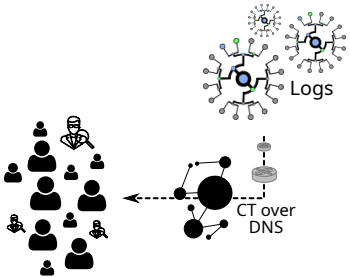


Solution (1/2)

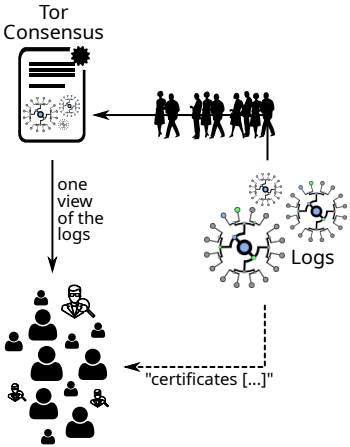
C2: Increased probability of split-view detection



Problem

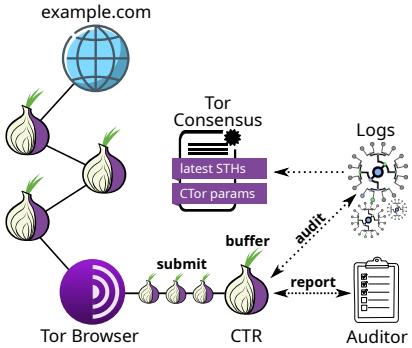


Solution (1/2)



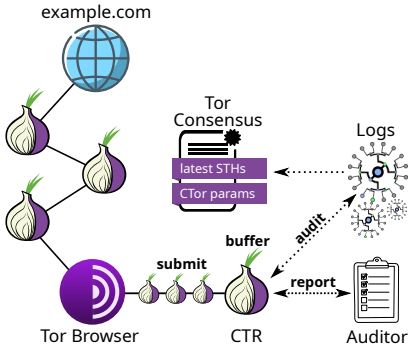
Solution (2/2)

C3: Improved detectability of website hijacks targeting Tor Browser



Solution (continued)

C3: Improved detectability of website hijacks targeting Tor Browser

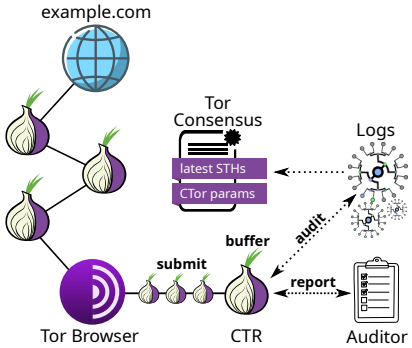


Attacker capabilities

- Vanilla Tor Browser threat model
- Plus zero-day on Tor Browser
- Plus operates enough logs

Solution (continued)

C3: Improved detectability of website hijacks targeting Tor Browser



Solution (continued)

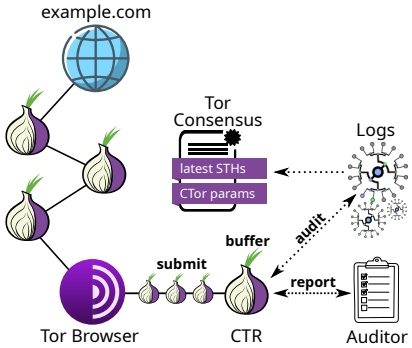
Attacker capabilities

- Vanilla Tor Browser threat model
- Plus zero-day on Tor Browser
- Plus operates enough logs

Security

- Break any of the four phases
- "Break" must go unnoticed

C3: Improved detectability of website hijacks targeting Tor Browser



Attacker capabilities

- Vanilla Tor Browser threat model
- Plus zero-day on Tor Browser
- Plus operates enough logs

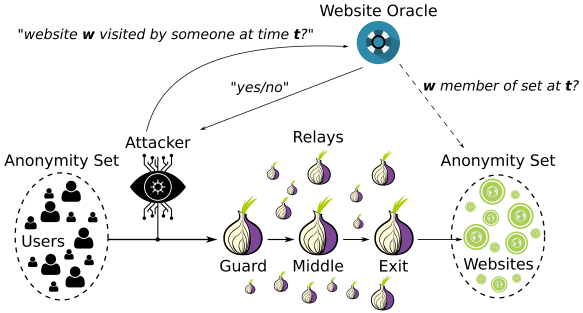
Security

- Break any of the four phases
- "Break" must go unnoticed

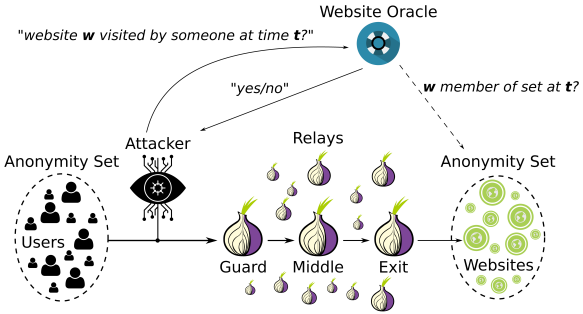
Solution (continued)

Gradual roll out, also use-cases relating to onion services

C4: An extension of the attacker model for website fingerprinting

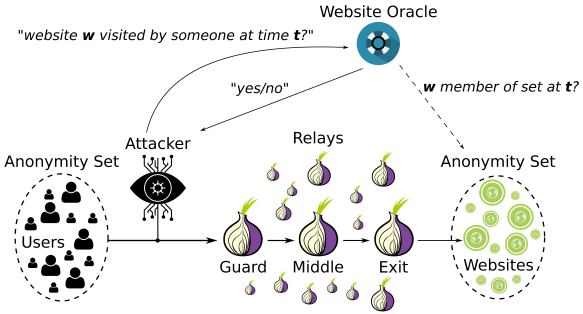


C4: An extension of the attacker model for website fingerprinting



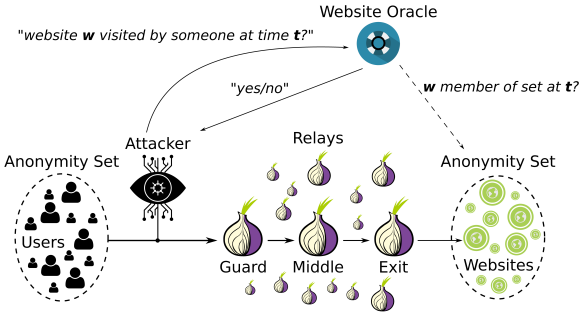
- Smaller destination anonymity set

C4: An extension of the attacker model for website fingerprinting



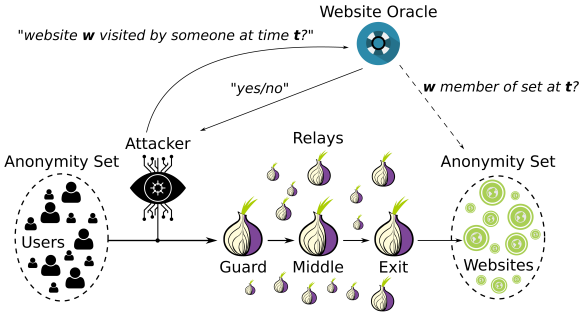
- Smaller destination anonymity set
- Eliminates most false positives for Alexa top-10k and beyond

C4: An extension of the attacker model for website fingerprinting



- Smaller destination anonymity set
- Eliminates most false positives for Alexa top-10k and beyond
- Gaining access to a website oracle?

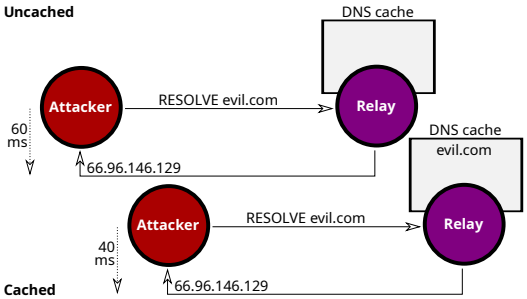
C4: An extension of the attacker model for website fingerprinting



- Smaller destination anonymity set
- Eliminates most false positives for Alexa top-10k and beyond
- Gaining access to a website oracle?

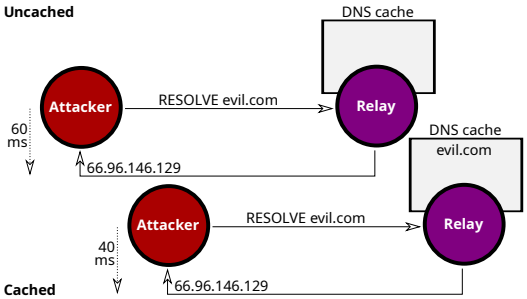
Certificate Transaprency logs, Certificate Authorities, ...

C5: Remotely-exploitable probing-attacks on Tor's DNS cache

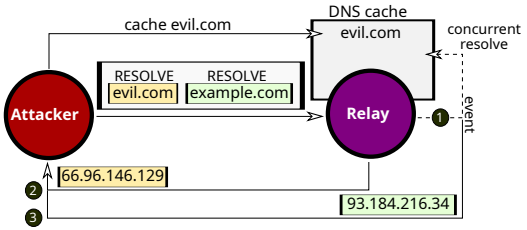


Timing attack

C5: Remotely-exploitable probing-attacks on Tor's DNS cache

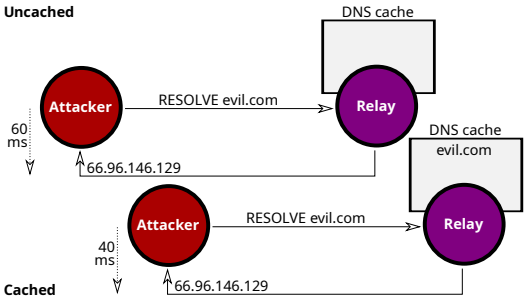


Timing attack

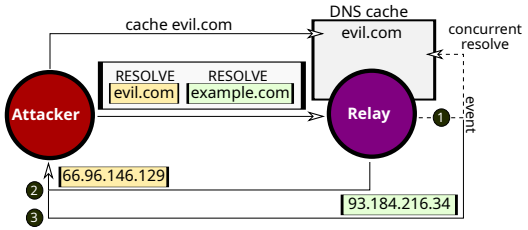


Timeless timing attack

C5: Remotely-exploitable probing-attacks on Tor's DNS cache



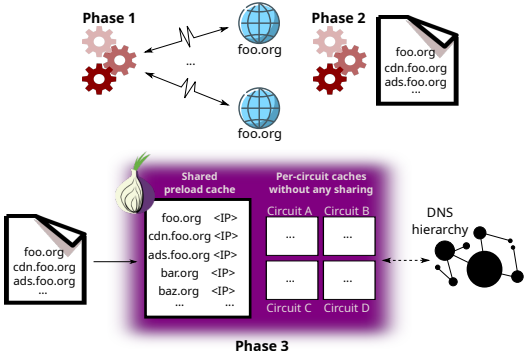
Timing attack



Timeless timing attack

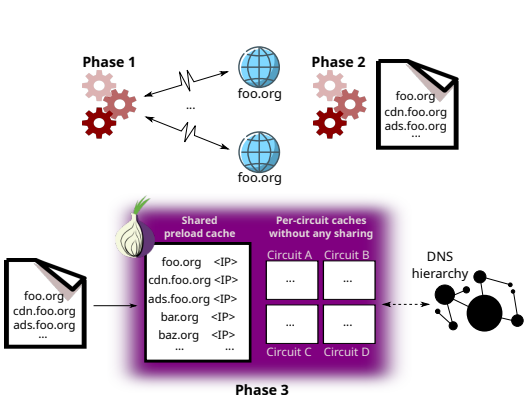
12M repetitions in the live Tor network, fully reliable attack prototype

C6: A redesign of Tor's DNS cache to defend against all (timeless) timing attacks

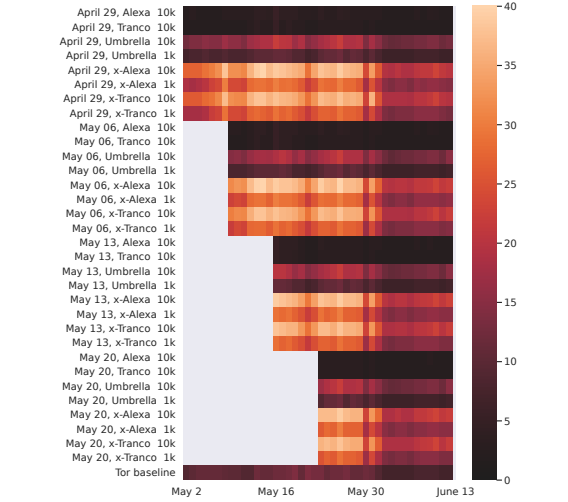


Preloaded DNS cache

C6: A redesign of Tor's DNS cache to defend against all (timeless) timing attacks

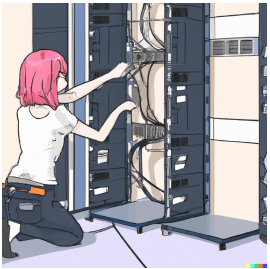


Preloaded DNS cache

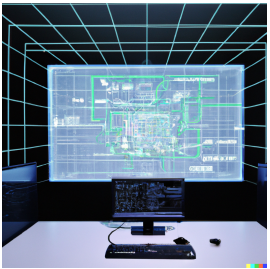


Summary of research methods

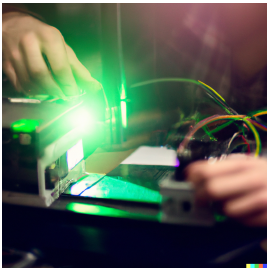
Threat modelling, proof sketching



Real-world measurements



Network simulation



Prototyping and evaluation

Take away

- Trust requirements can be reduced wrt. monitors and logs
- Certificate Transparency can work in Tor Browser's setting
- The website fingerprinting threat model could be stronger
- "On..."

Thank you

Paul Syverson
Linus Nordberg
Matthew Finkel
Tom Ritter
Tobias Pulls
Jonathan Vestin
Andreas Kassler
Toke Høiland-Jørgensen

Swedish Foundation for Strategic Research

Knowledge Foundation