PhD viva presentation

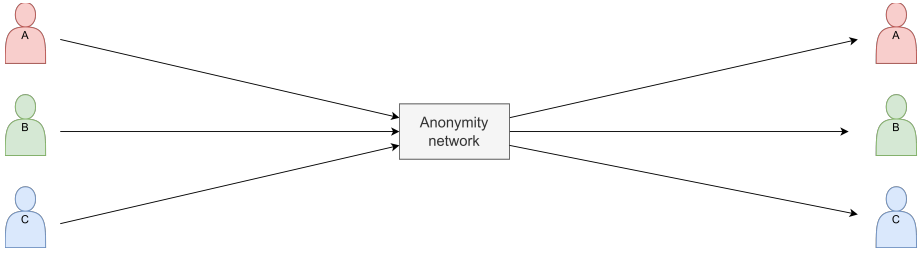
Killian Davitt

24.6.2024

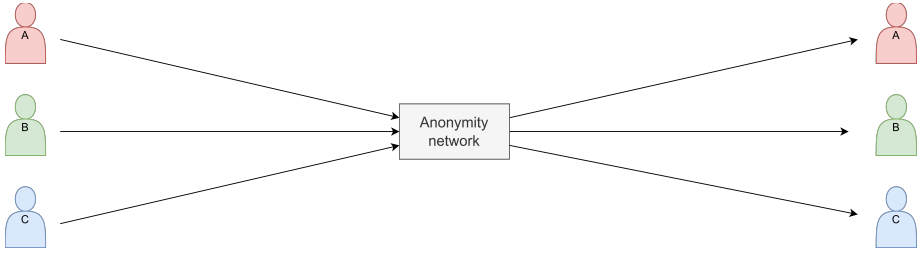
Motivation

- Anonymity can protect vulnerable users online
- Politically repressed, Ostracised communities, vulnerable persons
- Anonymity technologies need to be more accessible to non-technical people
- My 4 projects contribute to making anonymity tools more usable for all

Anonymity and usability

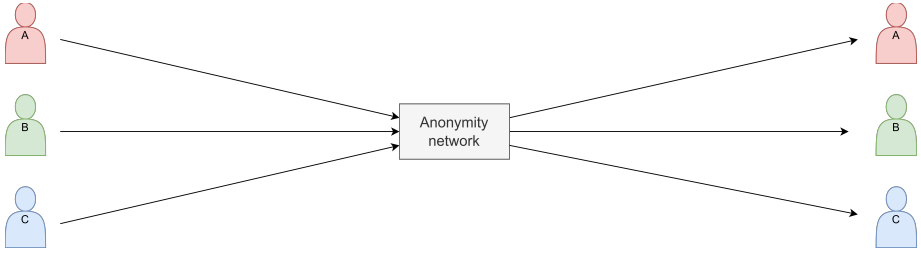


Anonymity and usability



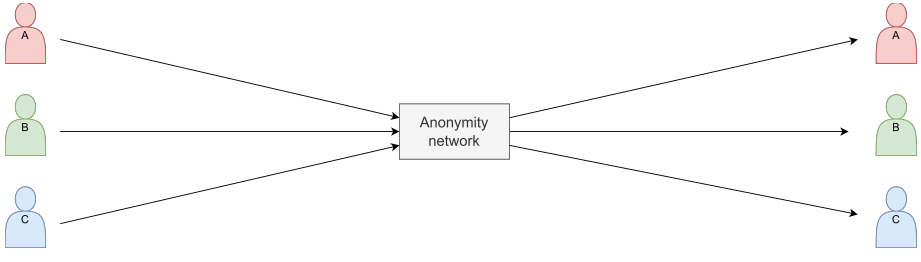
- A large number of participants is necessary for anonymity

Anonymity and usability



- A large number of participants is necessary for anonymity
- Usability of anonymity networks is essential

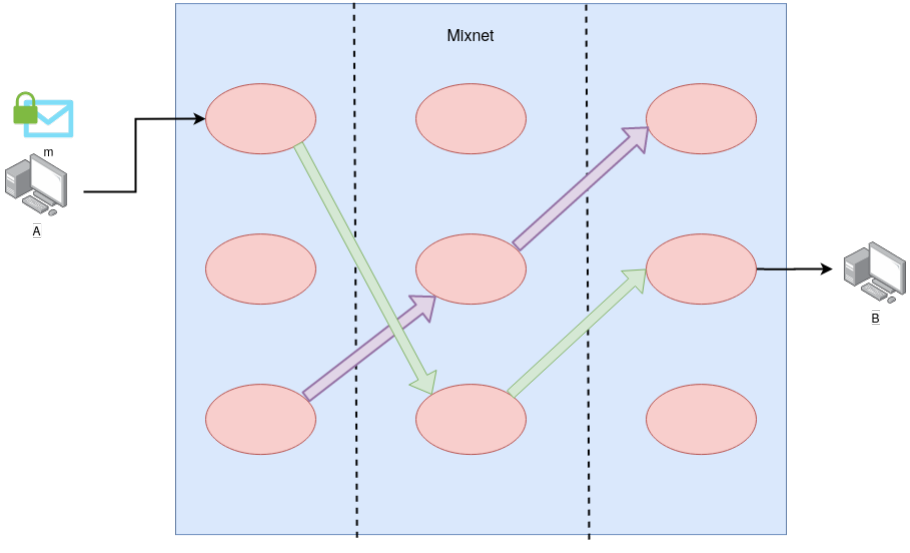
Anonymity and usability



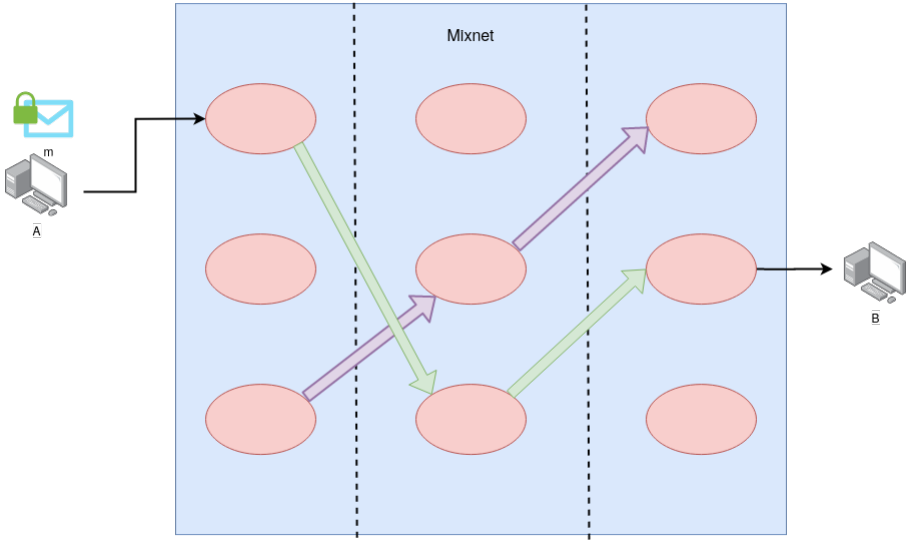
- A large number of participants is necessary for anonymity
- Usability of anonymity networks is essential
- People from different backgrounds and skill levels should be able to use them

Project 1 - Anonymous Collaboration: How Does Delay Affect User Experience?

Mixnets versus Tor

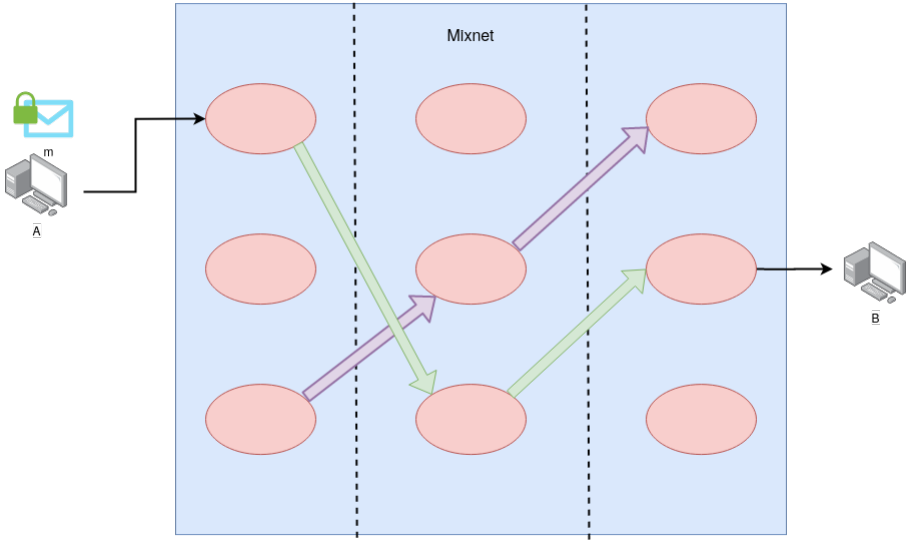


Mixnets versus Tor



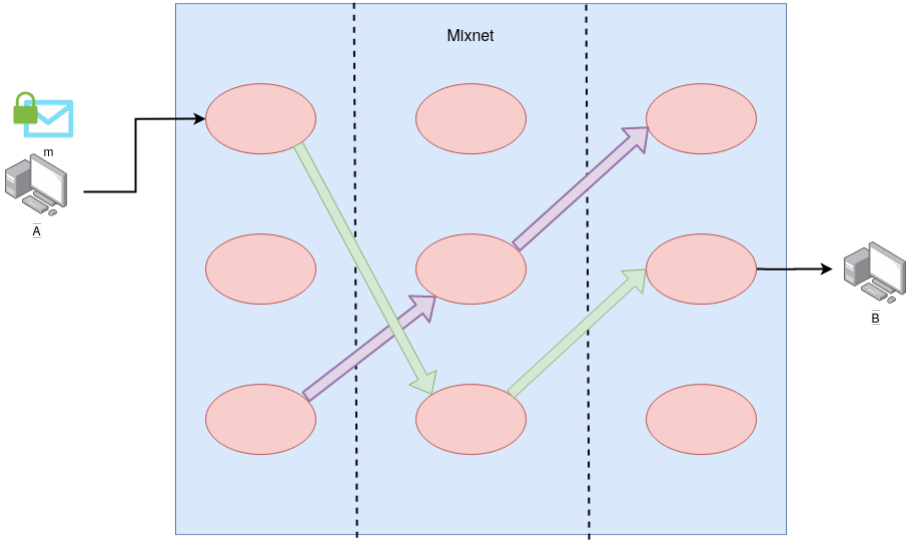
- Tor attempts to reduce latency as much as possible

Mixnets versus Tor



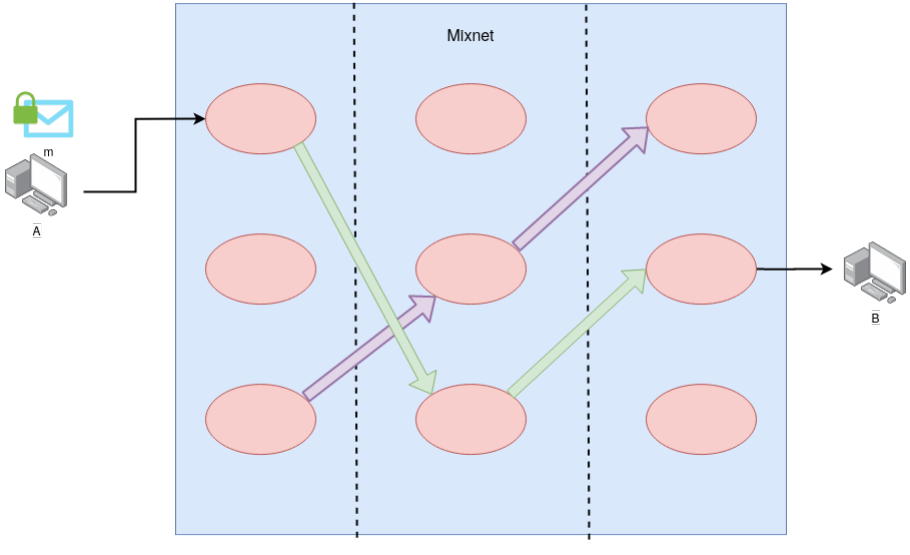
- Tor attempts to reduce latency as much as possible
- Mixnets include added latency by design

Mixnets versus Tor



- Tor attempts to reduce latency as much as possible
- Mixnets include added latency by design
- There is no prior work on users tolerance to delay in mixnets

Mixnets versus Tor



- Tor attempts to reduce latency as much as possible
- Mixnets include added latency by design
- There is no prior work on users tolerance to delay in mixnets
- My study is the first to research this

The collaboration task

The collaboration task

- Very general collaboration task that models conflicts between users

The collaboration task

- Very general collaboration task that models conflicts between users
- Set of 14 simple questions: analogous to document editing

The collaboration task

- Very general collaboration task that models conflicts between users
- Set of 14 simple questions: analogous to document editing
- Participants answers these questions in a collaboration with a "second user" which is simulated

The collaboration task

- Very general collaboration task that models conflicts between users
- Set of 14 simple questions: analogous to document editing
- Participants answers these questions in a collaboration with a "second user" which is simulated
- Mixnet delay is added between the participant and the simulated user

Delay levels

- Each participant repeats a collaboration task 5 times (+1 practice)
- Control: First scenario has no delay or 2nd user
- 1,000ms, 4,000ms, 7,000ms, 10,000ms

Compare completion time versus delay level

Compare completion time versus delay level

- Time taken to complete the task is measured

Compare completion time versus delay level

- Time taken to complete the task is measured
- Collaboration success: task completed faster than the control task

Compare completion time versus delay level

- Time taken to complete the task is measured
- Collaboration success: task completed faster than the control task
- Collaboration failure: task completed slower than the control task

Results

Delay (ms)	Mean Difference (s)	p–value
1000	−23.6	**<0.001*** **
4000	−19.7	**0.00249** **
7000	−13.7	0.085 05
10 000	−5.8	>0.9

** Significant below 0.01

* * * Significant below 0.005

Project 2 - HTTPS-Only Modes: what should they aim to do?

HTTPS-Only mode warning pages

HTTPS-Only Mode Alert

Secure Site Not Available

A HTTPS version of **mybank.com** is not available.
Learn More…

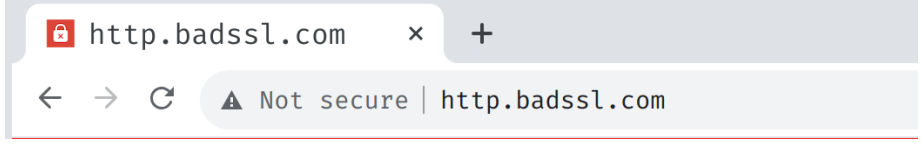
What could be causing this?

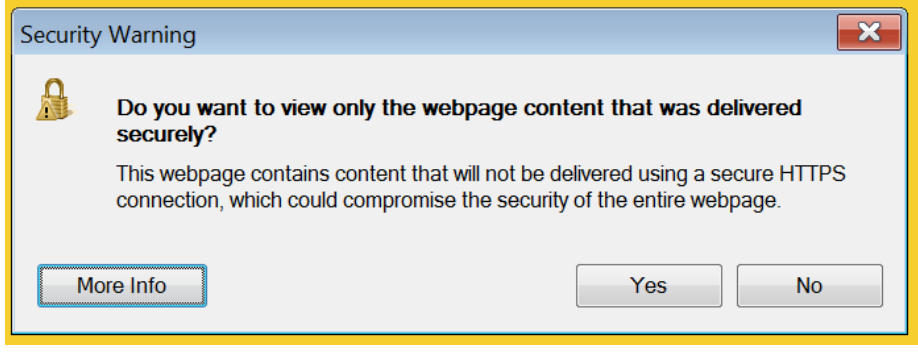
- Most likely, the web site simply does not support HTTPS.
- It's also possible that an attacker is involved.
- If you decide to visit the web site, you should not enter any sensitive information like passwords, emails, or credit card details.

If you continue, HTTPS-Only Mode will be turned off temporarily for this site.

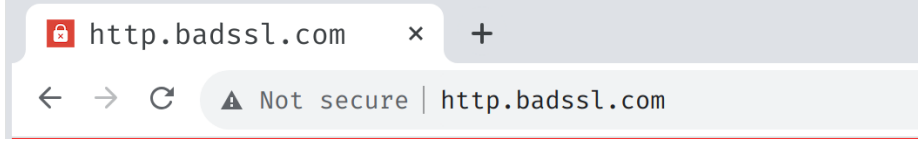
Continue to HTTP Site | Go Back

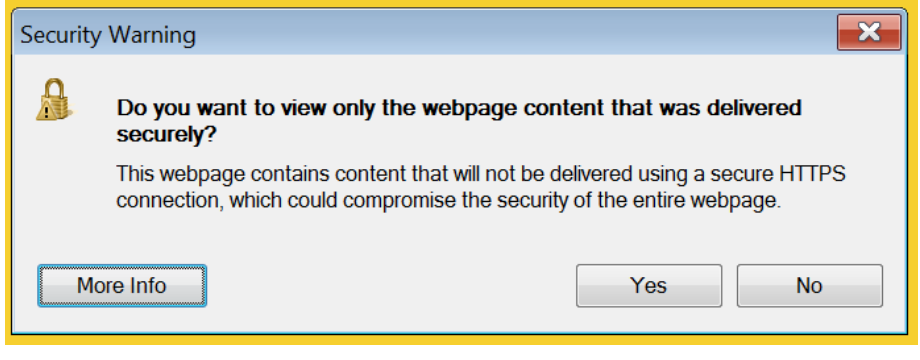
Progression of non-HTTPS warnings





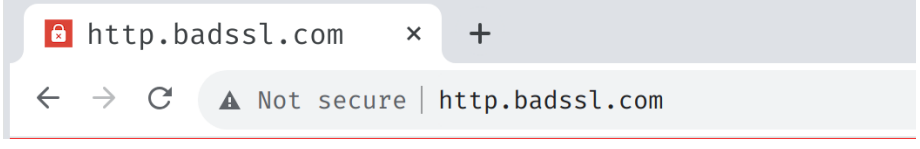
Progression of non-HTTPS warnings

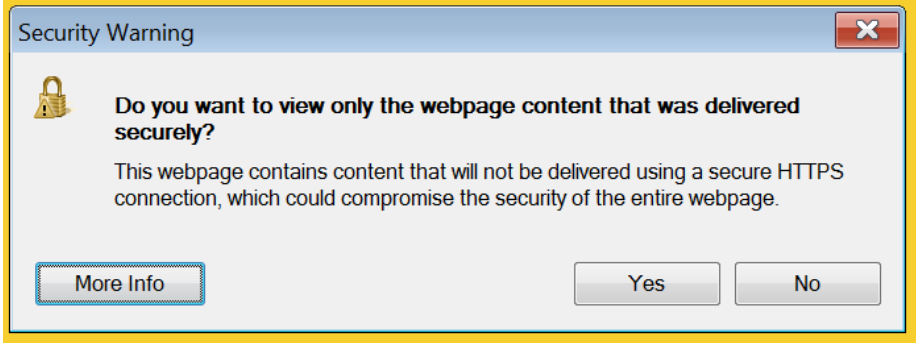




- Part of a progression of browser warnings

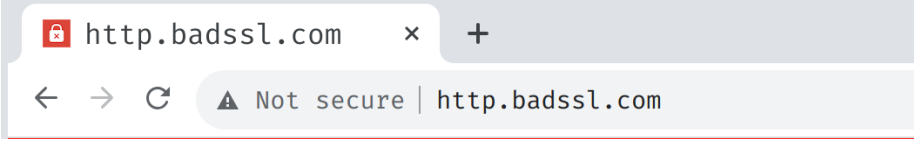
Progression of non-HTTPS warnings

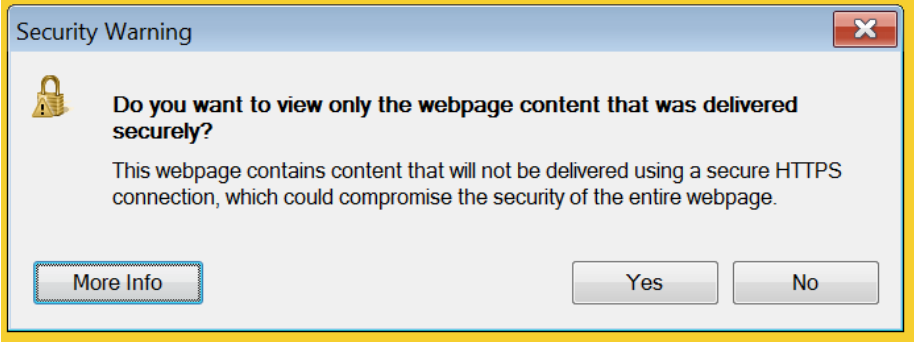




- Part of a progression of browser warnings
- The "lock", mixed-content warnings, de-ranking google results

Progression of non-HTTPS warnings





- Part of a progression of browser warnings
- The "lock", mixed-content warnings, de-ranking google results
- This the most intrusive warning against non-HTTPS websites yet

How should users react to these pages?

How should users react to these pages?

- HTTPS-Only modes have not yet been studied in the literature

How should users react to these pages?

- HTTPS-Only modes have not yet been studied in the literature
- non-HTTPS websites can be safe

How should users react to these pages?

- HTTPS-Only modes have not yet been studied in the literature
- non-HTTPS websites can be safe
- Different type of warning to other browser warning pages (e.g. SSL)

How should users react to these pages?

- HTTPS-Only modes have not yet been studied in the literature
- non-HTTPS websites can be safe
- Different type of warning to other browser warning pages (e.g. SSL)
- My survey is the first piece of work to discuss how they should be used

Survey

- 28 Participants
- Tor Experts
- Participants were asked their thoughts on risk from non-HTTPS websites
    - What factors effect it
    - How they think others understand it
    - What they think of current warning pages

Results

- Data showed a number of themes discussed by participants

Context

- The type of website is crucial when determining safety
- Banking without HTTPS: dangerous
- Checking opening hours: safe

User Agency

- Should users be given the choice?
- Banning non-HTTPS websites would be safe, but also annoying

Content Integrity

- Current warning pages do not discuss content integrity
- Not discussed by any warnings
- Users may not understand this concept

Specific Risks

- Current warning pages do not discuss any specific examples of risk
- E.g. If you enter your credit card details on this website, your money could be stolen

Lack of Tor specific discussion

- Users of Tor face different risk from regular web users
- Warning pages should highlight this

Project 3 - Creating New Warning Pages for HTTPS-Only Modes in Tor Browser

Improving HTTPS Only mode warning pages

- This project uses the results from the previous chapter to produce an improved HTTPS Only Mode warning page

Context warning

HTTPS-Only Mode Alert

Secure Site Not Available

A HTTPS version of **mybank.com** is not available.
Learn More…

What should I do about this?

- If you visit this site to log in to an account, do shopping, or anything private, you are at risk
- If you read this site without entering personal details, you are less at risk
- Do not enter any sensitive information like passwords, email addresses, or credit card details.
- Any information you enter could be stolen by an attacker.

If you continue, HTTPS-Only Mode will be turned off temporarily for this site.

Continue to Less Secure Site | Go Back

- Warns user to decide based on the type of website

Popularity warning

HTTPS-Only Mode Alert

Secure Site Not Available

A HTTPS version of **mybank.com** is not available.
Learn More…

What should I do about this?

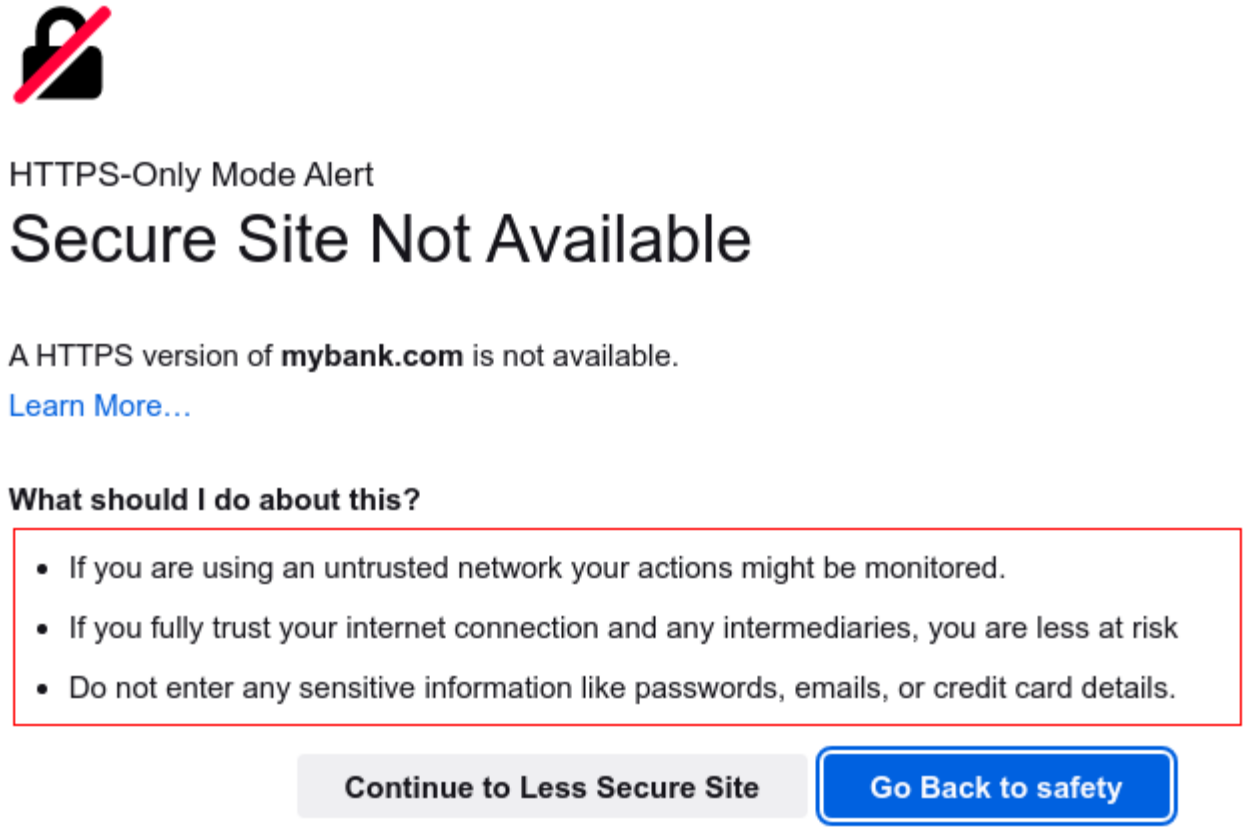
- If this is a well known, popular site, an attacker is likely involved. Do not visit the website.
- If this is not a popular, professional website, you are less at risk.
- A website you trust is more likely to be risky, for example a bank or financial institution.
- Do not enter any sensitive information like passwords, emails, or credit card details.

If you continue, HTTPS-Only Mode will be turned off temporarily for this site.

Continue to Less Secure Site **Go Back**

- Warns user to not proceed if website is very popular or is a large

Tor warning



- Warns the user that they are more vulnerable while using Tor

Results

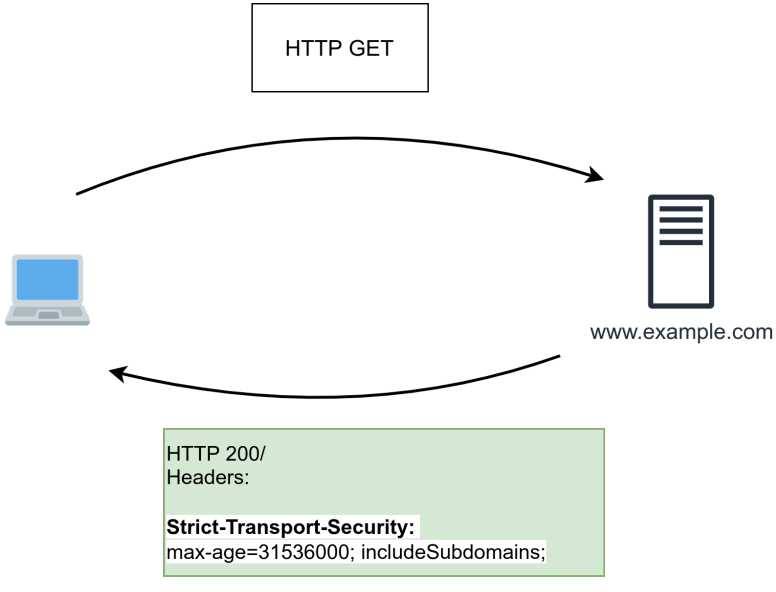
Warning	Correct	Incorrect	Total	Test Statistic	p-value
Control	1989	1011	3000		
Popularity	2037	927	2964	3.8862	**0.0487***
Context	1990	1016	3006	0.0029	0.9570
Tor	1998	996	2994	0.1077	0.7428

Conclusion

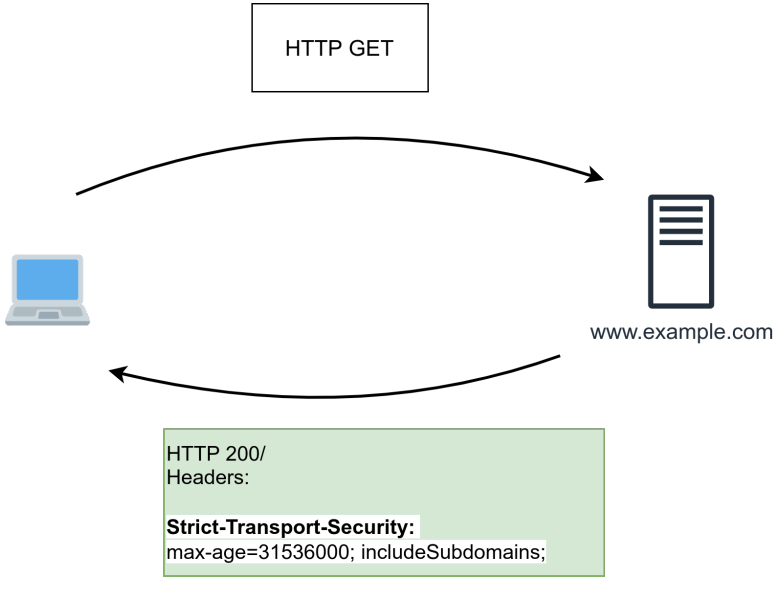
- The techniques explored can offered improved results
- The project provides the first quantitative evaluation of any HTTPS Only mode warning page

Project 4 - CoStrictTor: Bringing HSTS to Tor browser

HSTS

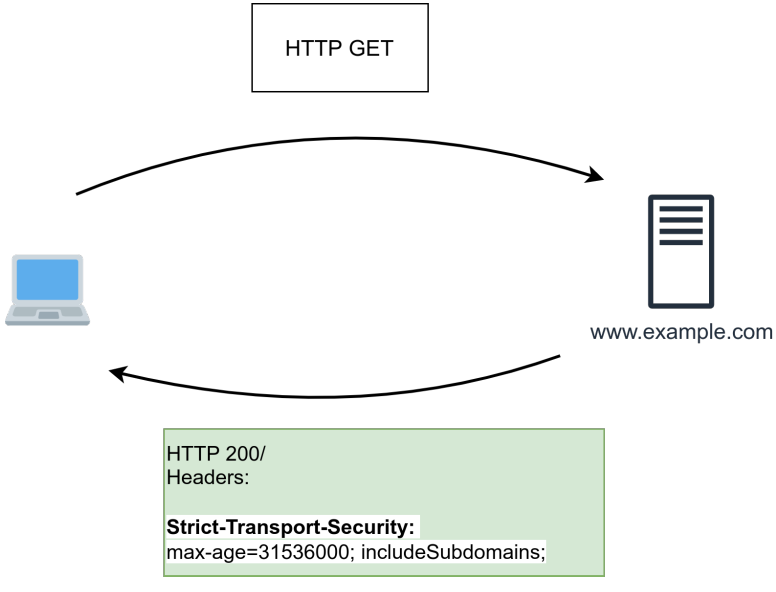

HTTP GET
www.example.com
HTTP 200/
Headers:
Strict-Transport-Security:
max-age=31536000; includeSubdomains;

HSTS



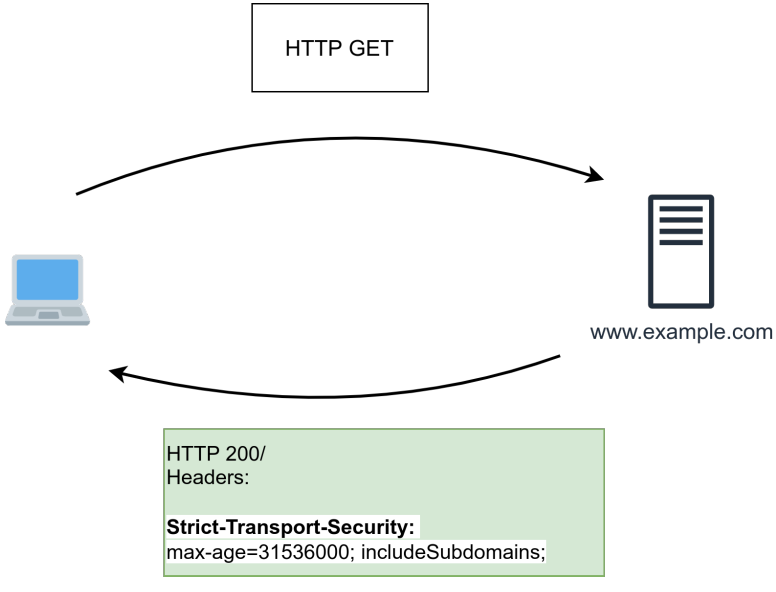
- HTTP header

HSTS



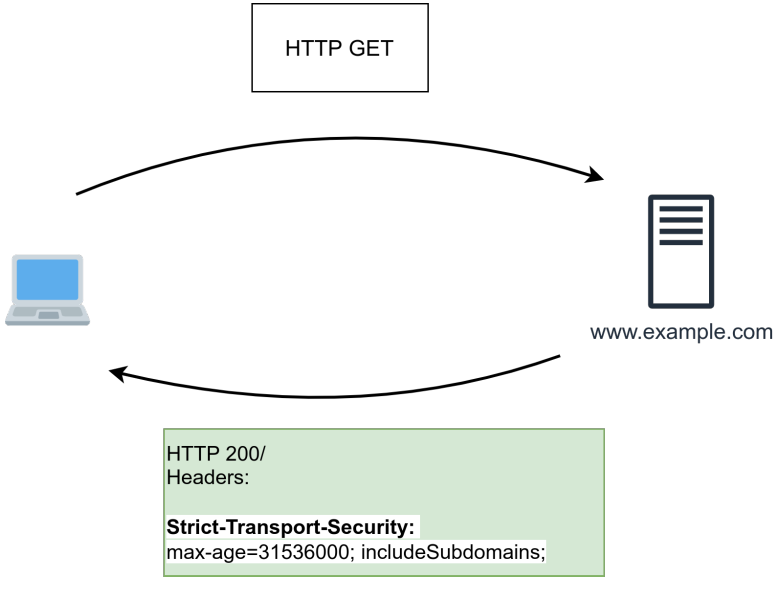
- HTTP header
- "Always enforce https from now on"

HSTS



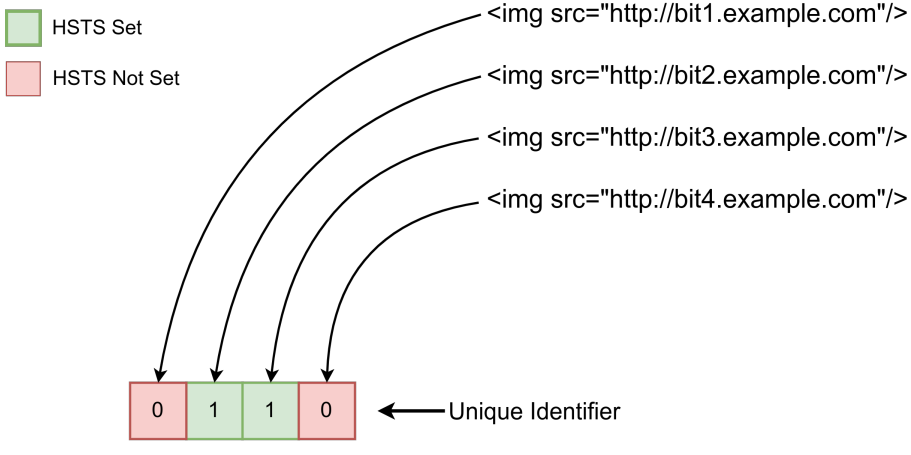
- HTTP header
- "Always enforce https from now on"
- Reduces MITM Attacks!

HSTS

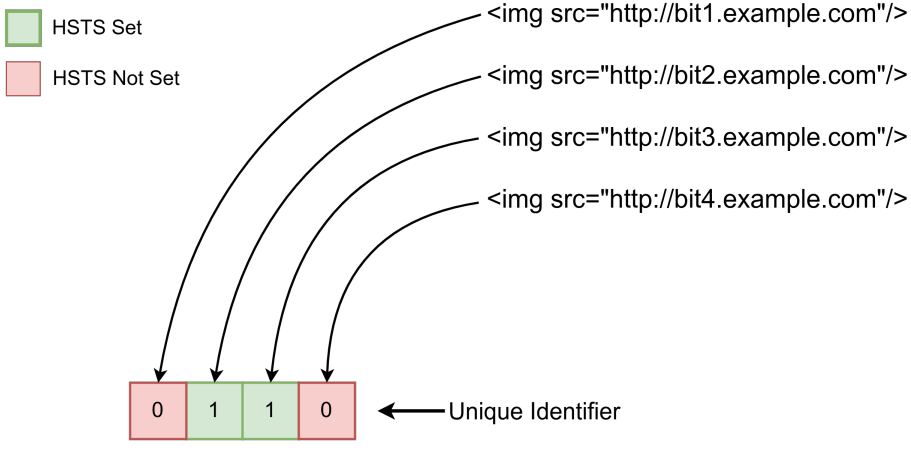


- HTTP header
- "Always enforce https from now on"
- Reduces MITM Attacks!
- Used by 20% of top sites

HSTS is exploited for Tracking

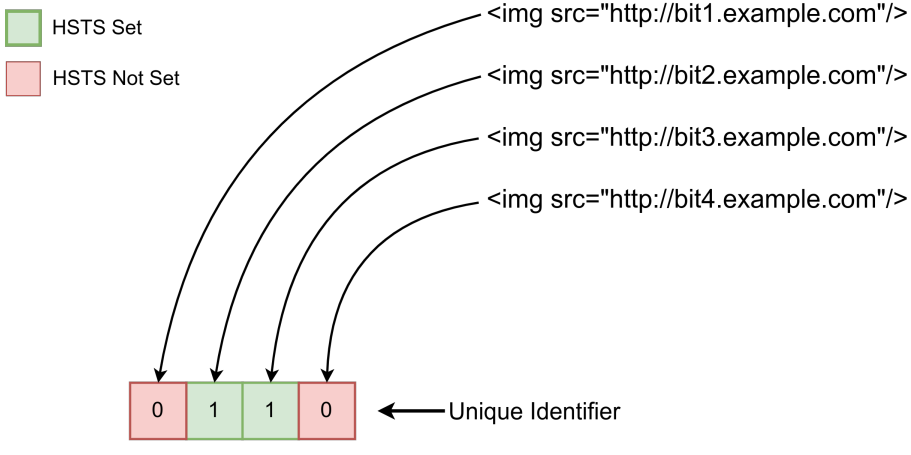


HSTS is exploited for Tracking



- Site selectively activates HSTS on the "bits"

HSTS is exploited for Tracking



- Site selectively activates HSTS on the "bits"
- Your browser reports this back on subsequent visits

Tor Browser

Tor Browser

- Tor Browser disables HSTS by default

Tor Browser

- Tor Browser disables HSTS by default
- Prevents tracking

Tor Browser

- Tor Browser disables HSTS by default
- Prevents tracking
- But loses out on security guarantees

Our Protocol

Our Protocol

- Our protocol sources HSTS data from users

Our Protocol

- Our protocol sources HSTS data from users
- Meaning: Tor Browser users share the same HSTS data

Our Protocol

- Our protocol sources HSTS data from users
- Meaning: Tor Browser users share the same HSTS data
- Adaptation of RAPPOR [1]

[1] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response

RAPPOR

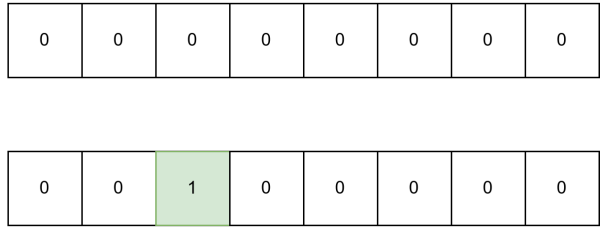
- Uses randomised response to introduce differential privacy
- Encode submissions into a bloom filter, perturb randomly

Bloom filters

Set Insertion

hash("*www.google.com*") = 1110101

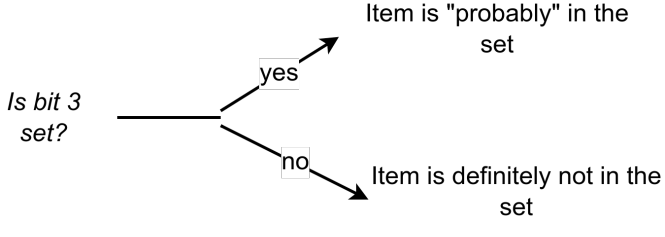
117 mod 8 = 5



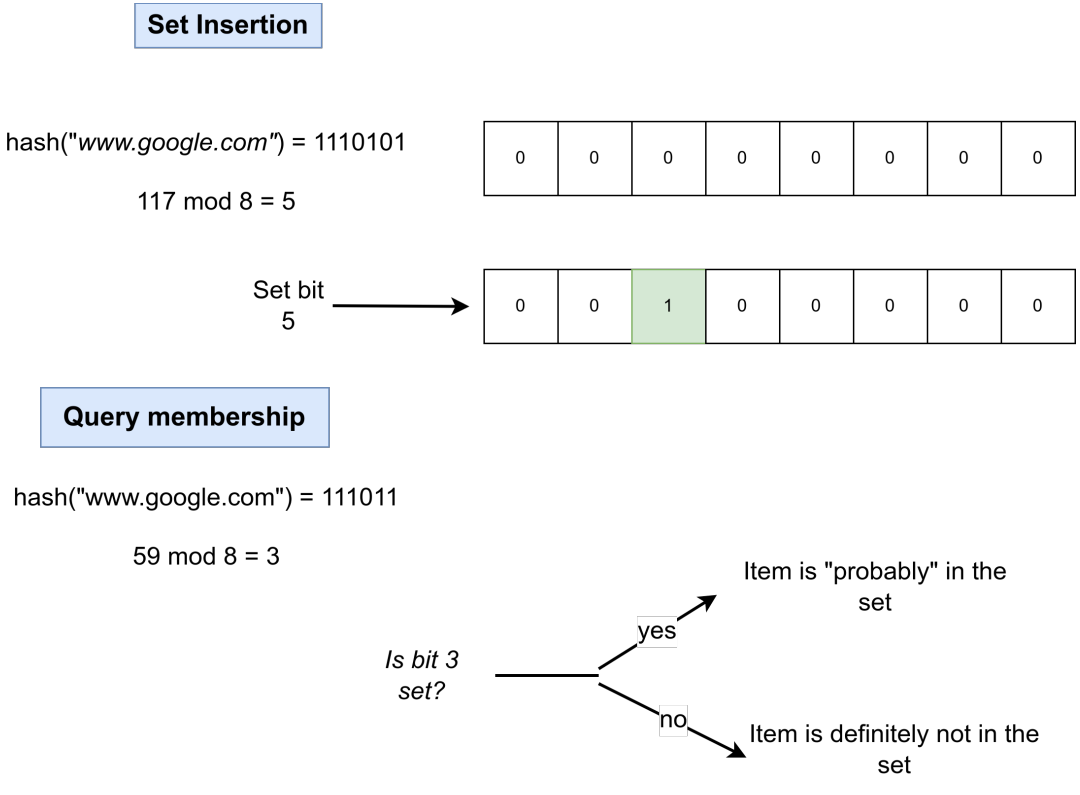
Query membership

hash("www.google.com") = 111011

59 mod 8 = 3

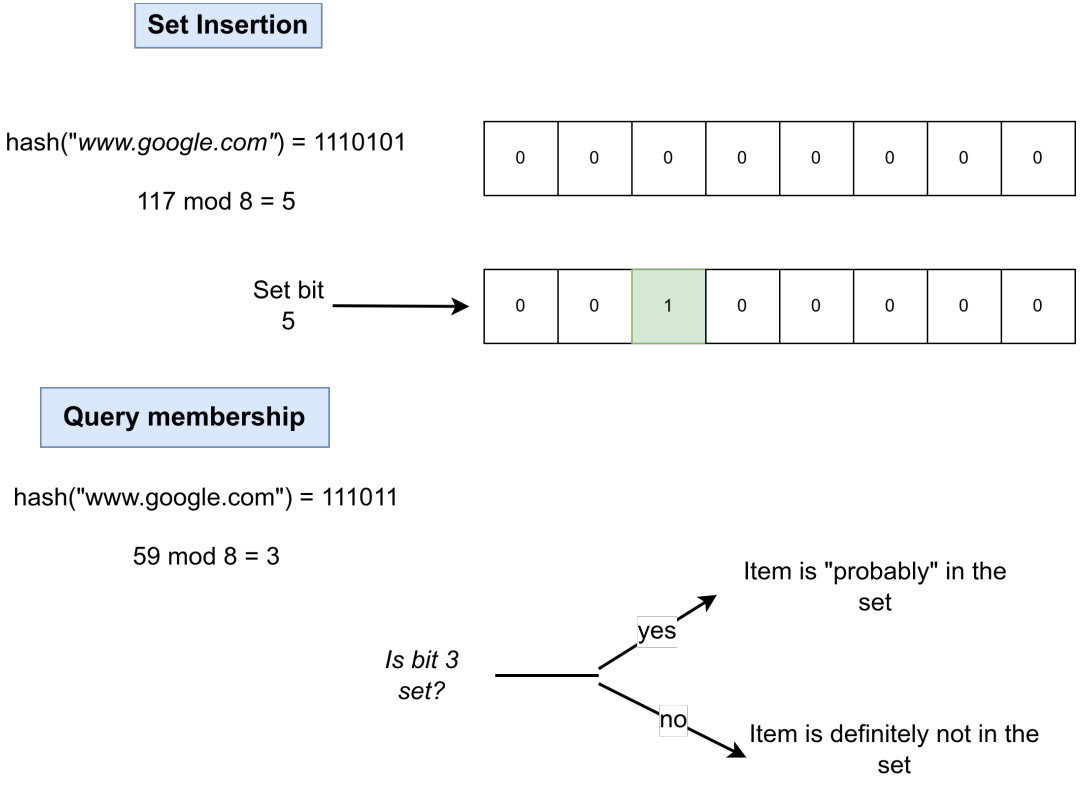


Bloom filters



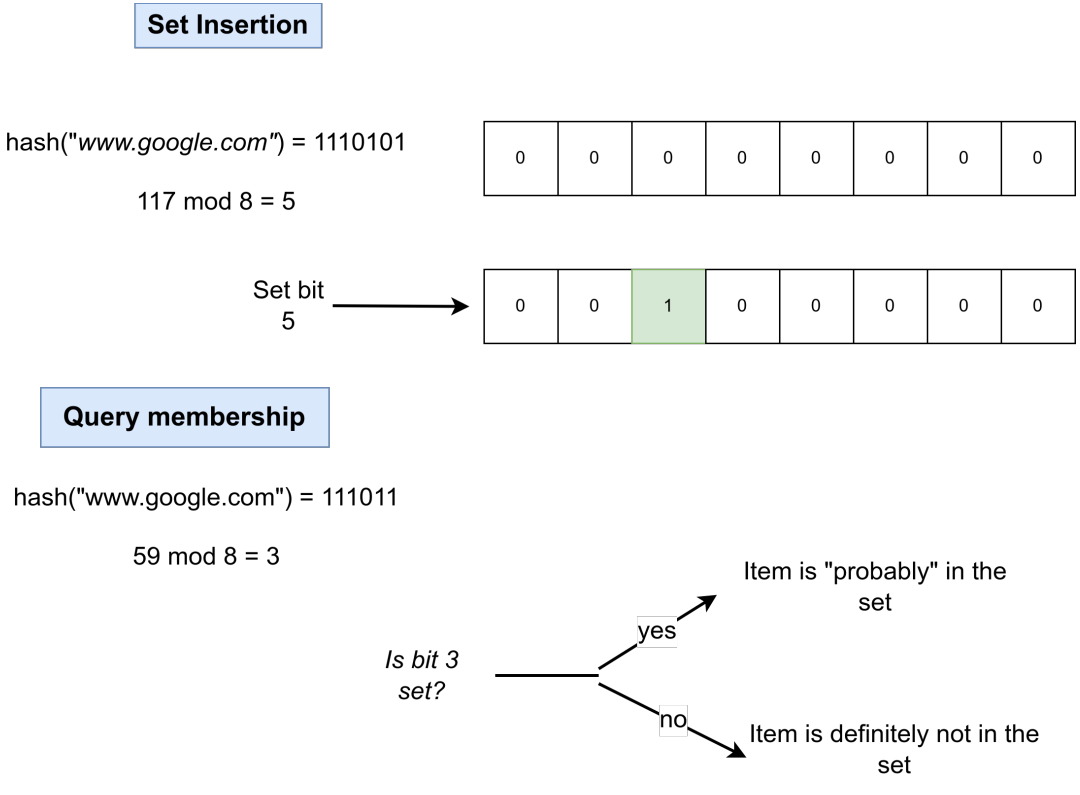
- Probabilistically correct!

Bloom filters



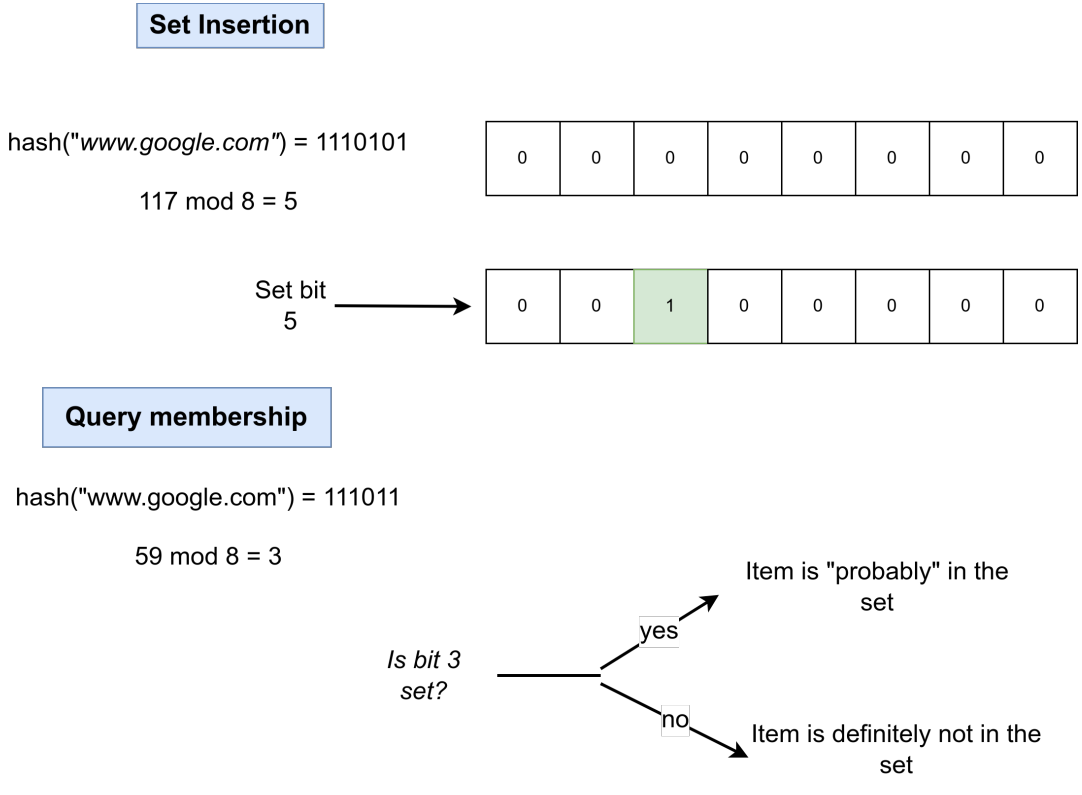
- Probabilistically correct!
- Inherent false positive rate

Bloom filters



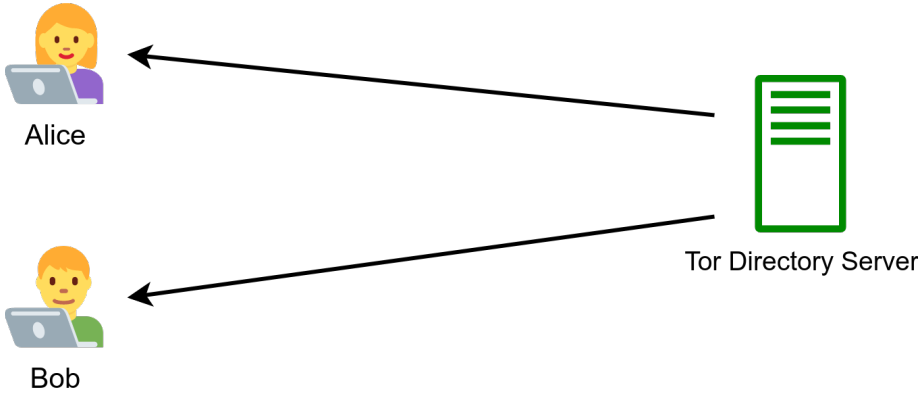
- Probabilistically correct!
- Inherent false positive rate
- We can also set counts:

Bloom filters



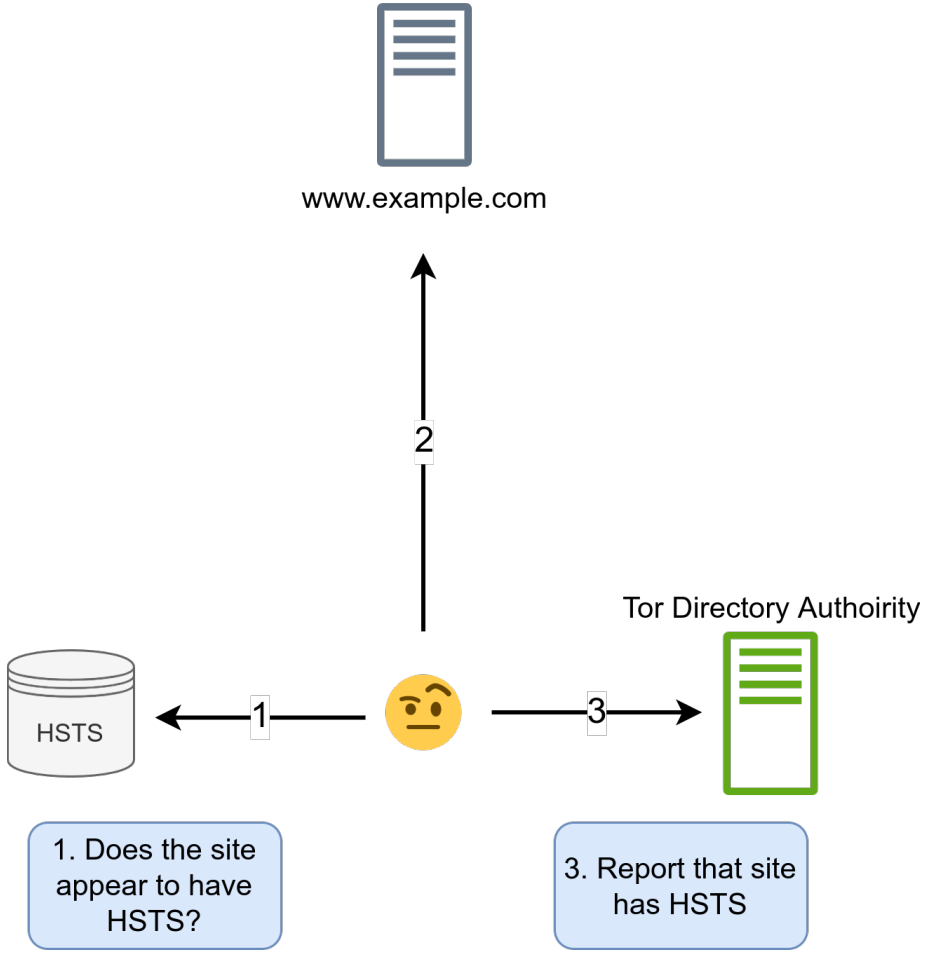
- Probabilistically correct!
- Inherent false positive rate
- We can also set counts:
- bit -> int

Distributing bloom filter data:



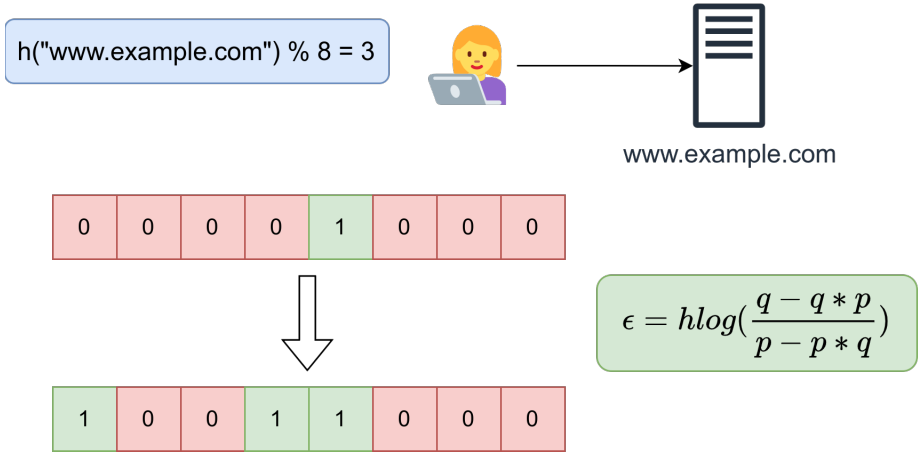
- Users periodically retrieve data from Tor directory server
- Data blob consisting of 2 bloom filters. Total size approx 130KB

Loading a website...



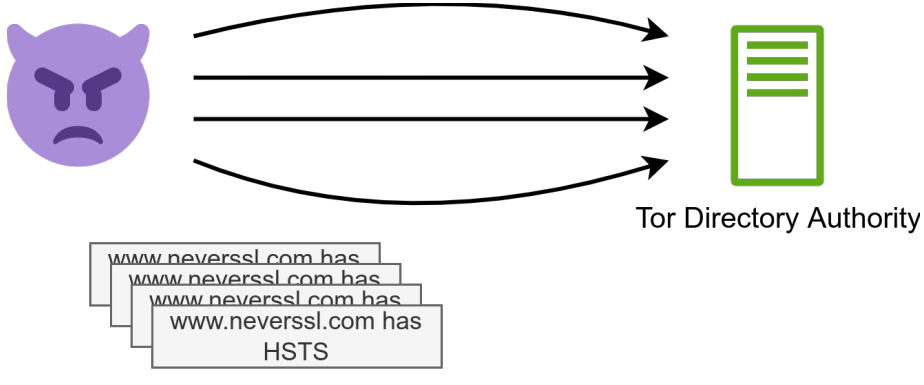
- User navigates to example.com
- before sending the request, check the count of www.example.com in the bloom filter
- If the count exceeds threshold, assume HSTS and force HTTPS
- Otherwise, disregard protocol and load www.example.com as normal
- If the site reports HSTS, report that to server

Privacy guarantees



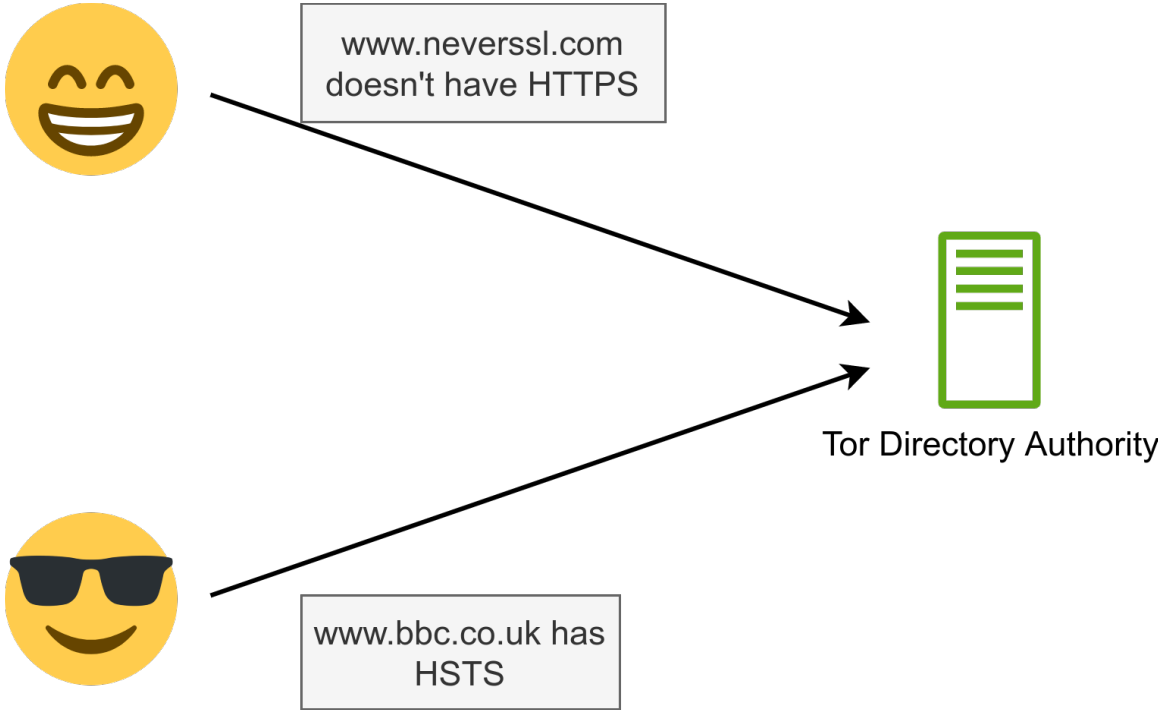
- Each bit is perturbed according to privacy parameters p,q
- $0 \leq p, q \leq 1$
- report a true 1 at probability q
- report a false 1 at probability p

Denial of Service

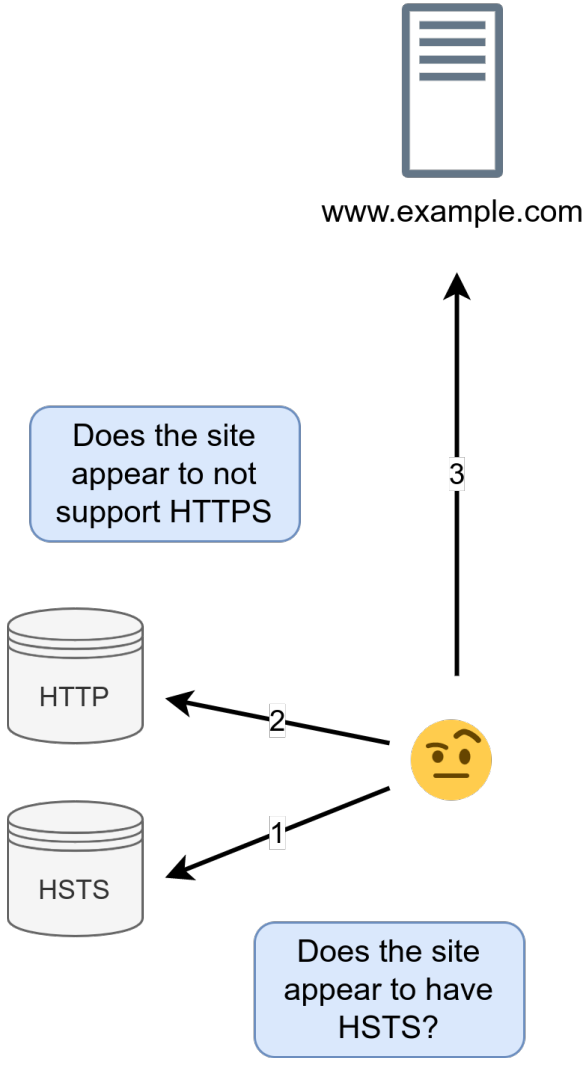


- Submit lots of incorrect entries!
- Blocks users from accessing the site!

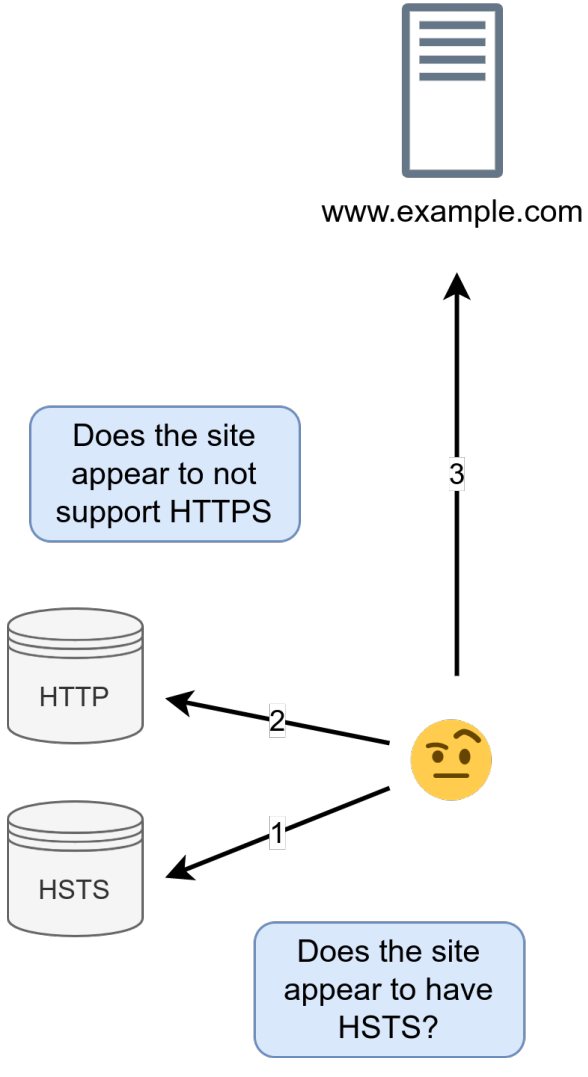
Report sites with HTTP only!



Loading a website...

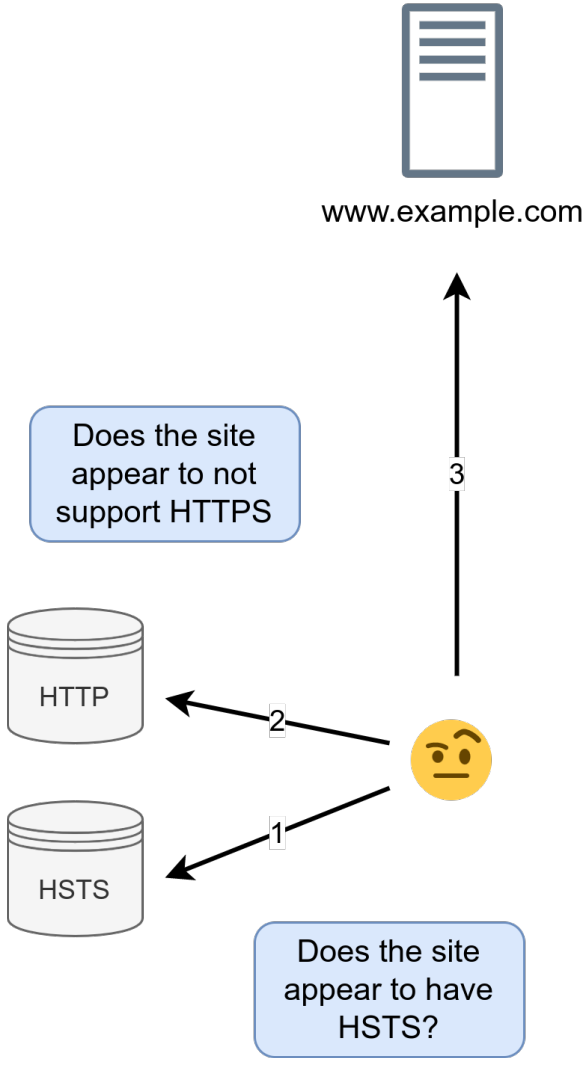


Loading a website...



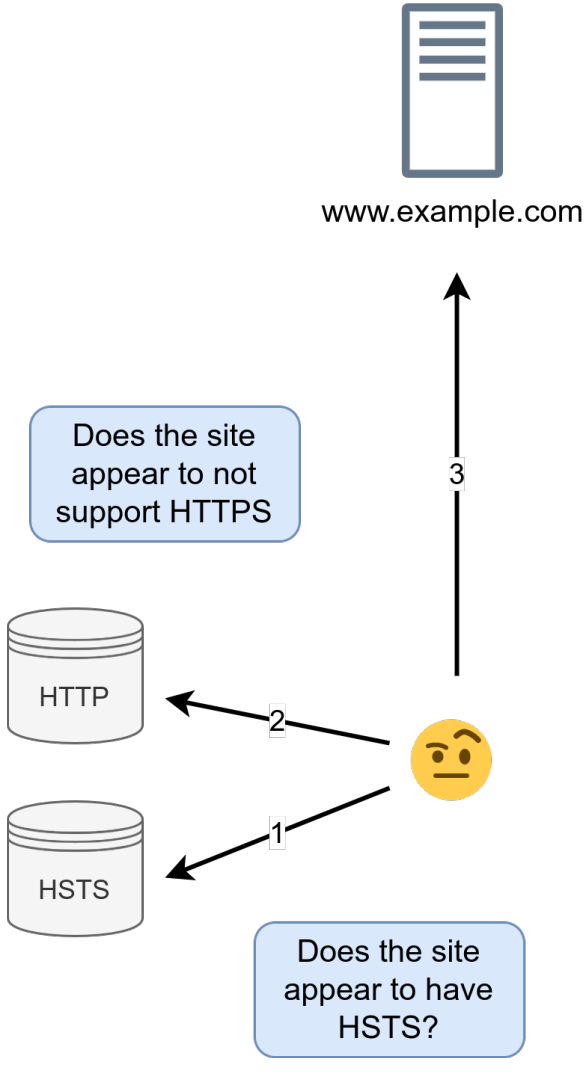
- After detecting HSTS, we also check if a site appears in the register of HTTP sites

Loading a website...



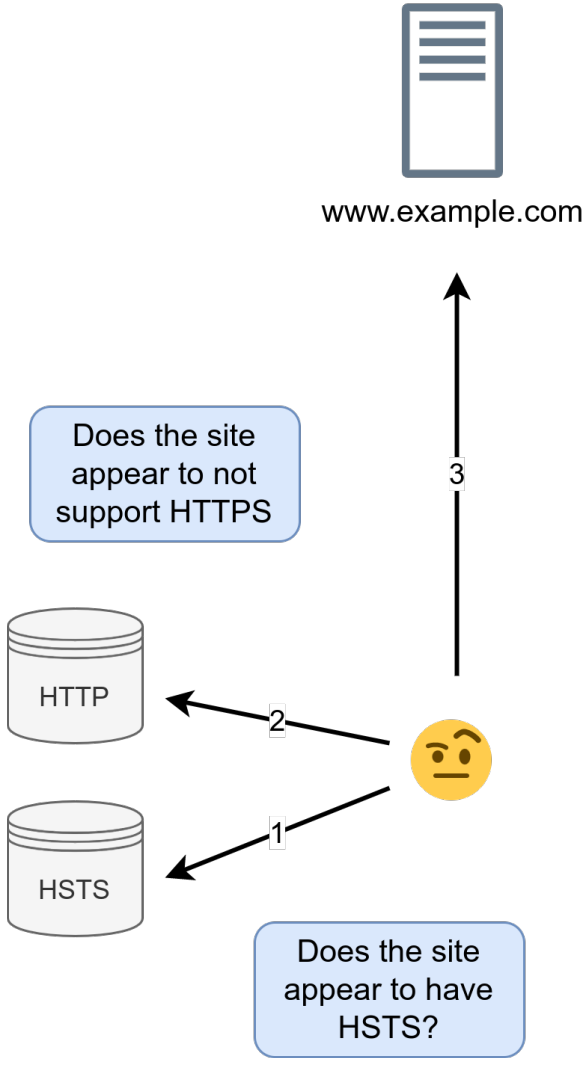
- After detecting HSTS, we also check if a site appears in the register of HTTP sites
- By definition sites without HTTPS, do not have HSTS

Loading a website...



- After detecting HSTS, we also check if a site appears in the register of HTTP sites
- By definition sites without HTTPS, do not have HSTS
- If a site appears in both, something has gone wrong

Loading a website...



- After detecting HSTS, we also check if a site appears in the register of HTTP sites
- By definition sites without HTTPS, do not have HSTS
- If a site appears in both, something has gone wrong
- Warn the user, but don't restrict their access to the site

Results

Results

- The accuracy of results is based off number of submissions

Results

- The accuracy of results is based off number of submissions
- More submissions -> more websites accurately detected

Results

- The accuracy of results is based off number of submissions
- More submissions -> more websites accurately detected
- Assuming widespread use in Tor Browser, we can accurately report on **10,000 websites**

Results

- The accuracy of results is based off number of submissions
- More submissions -> more websites accurately detected
- Assuming widespread use in Tor Browser, we can accurately report on **10,000 websites**
- We can achieve **ε of approx 7**

Results

- The accuracy of results is based off number of submissions
- More submissions -> more websites accurately detected
- Assuming widespread use in Tor Browser, we can accurately report on **10,000 websites**
- We can achieve **ε of approx 7**
- This will improve with ever increasing HTTPS adoption

Results

- The accuracy of results is based off number of submissions
- More submissions -> more websites accurately detected
- Assuming widespread use in Tor Browser, we can accurately report on **10,000 websites**
- We can achieve **ε of approx 7**
- This will improve with ever increasing HTTPS adoption
- Reducing man-in-the-middle attacks on Tor Browser

Conclusion

Conclusion

- I completed 4 different projects enhancing the usability of anonymity networks

Conclusion

- I completed 4 different projects enhancing the usability of anonymity networks
- Many of these improvements are applicable to both Tor and Mixnets

Conclusion

- I completed 4 different projects enhancing the usability of anonymity networks
- Many of these improvements are applicable to both Tor and Mixnets
- Improvements to the user experience attracts more users from diverse backgrounds improving the size and diversity of the anonymity set