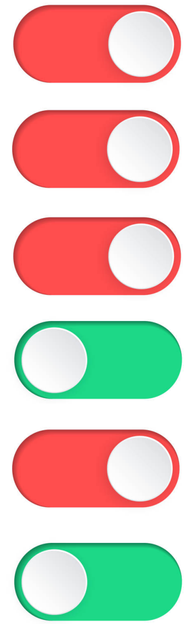
EPFL MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY CISPA HELMHOLTZ-ZENTRUM FÜR INFORMATIONSSICHERHEIT

Double-Edged Shield

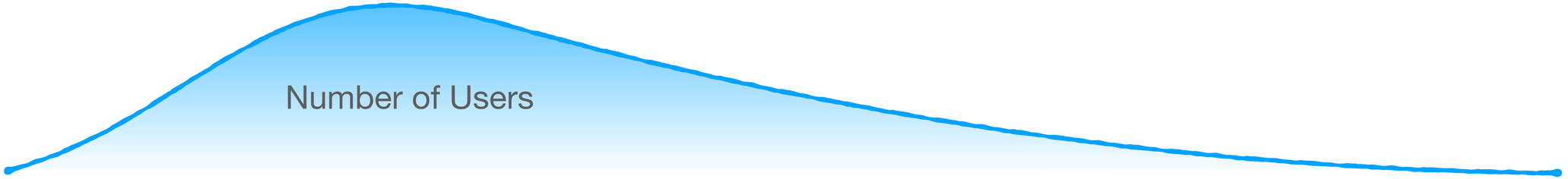
On the Fingerprintability of Customized Ad Blockers

34TH USENIX SECURITY SYMPOSIUM

Saiid El Hajj Chehade (EPFL), Ben Stock (CISPA), Carmela Troncoso (EPFL & MPI-SP)

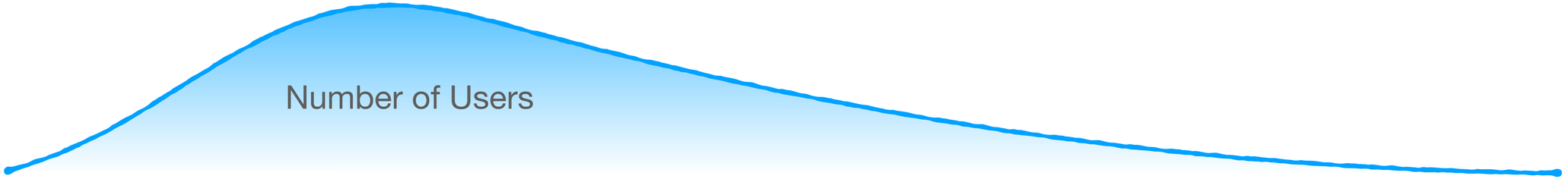


Privacy online



Web Surfer

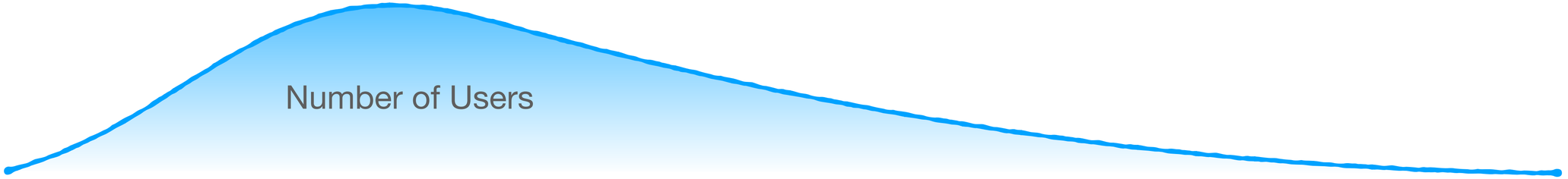
Privacy online



Web Surfer

Concerned about Privacy

Privacy online

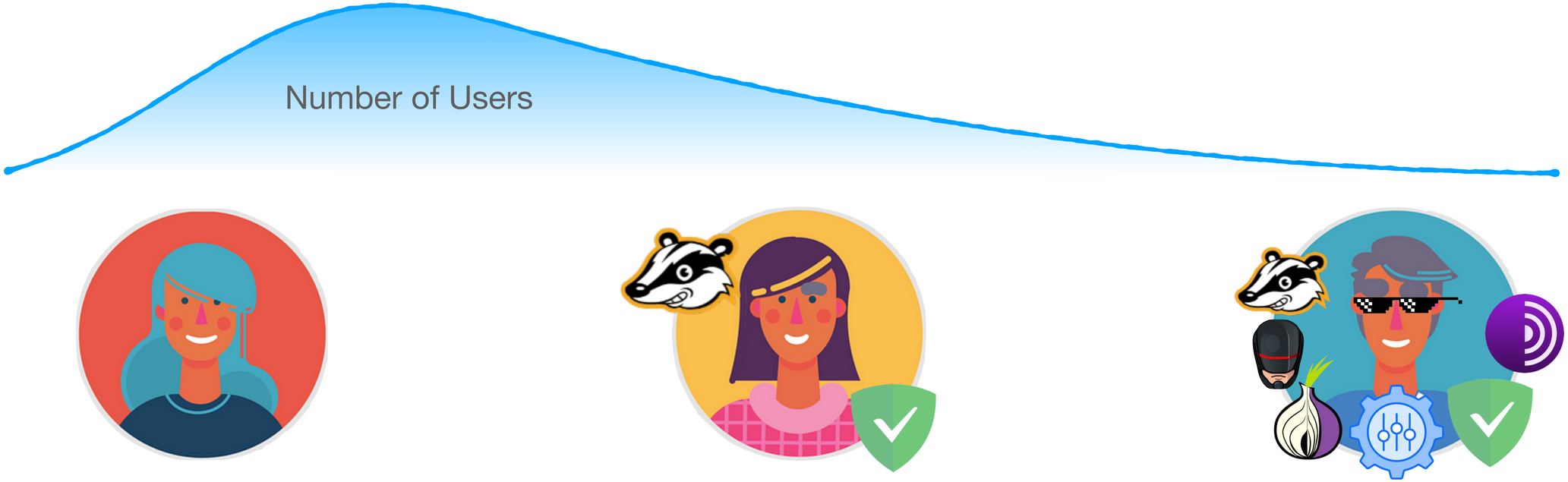


Web Surfer

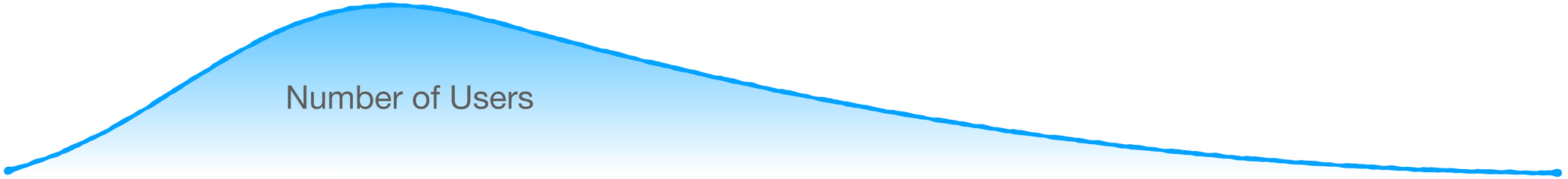
Concerned about Privacy

Privacy Power Users

Privacy online



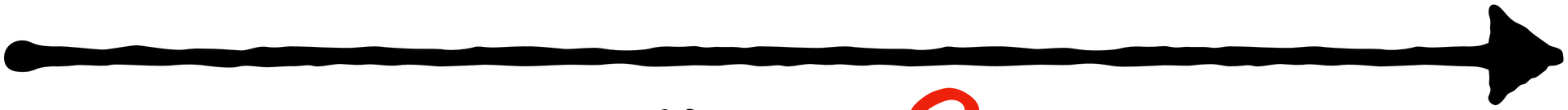
Privacy online



Web Surfer

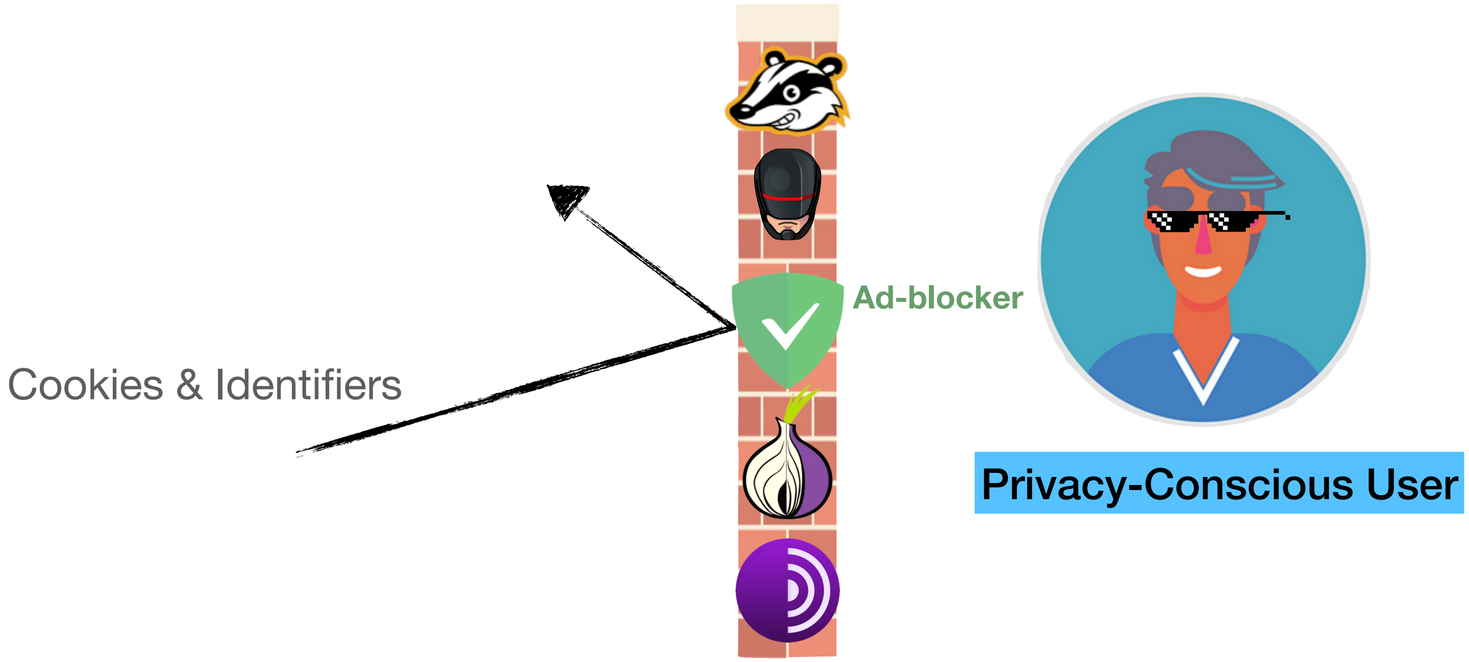
Concerned about Privacy

Privacy Power Users

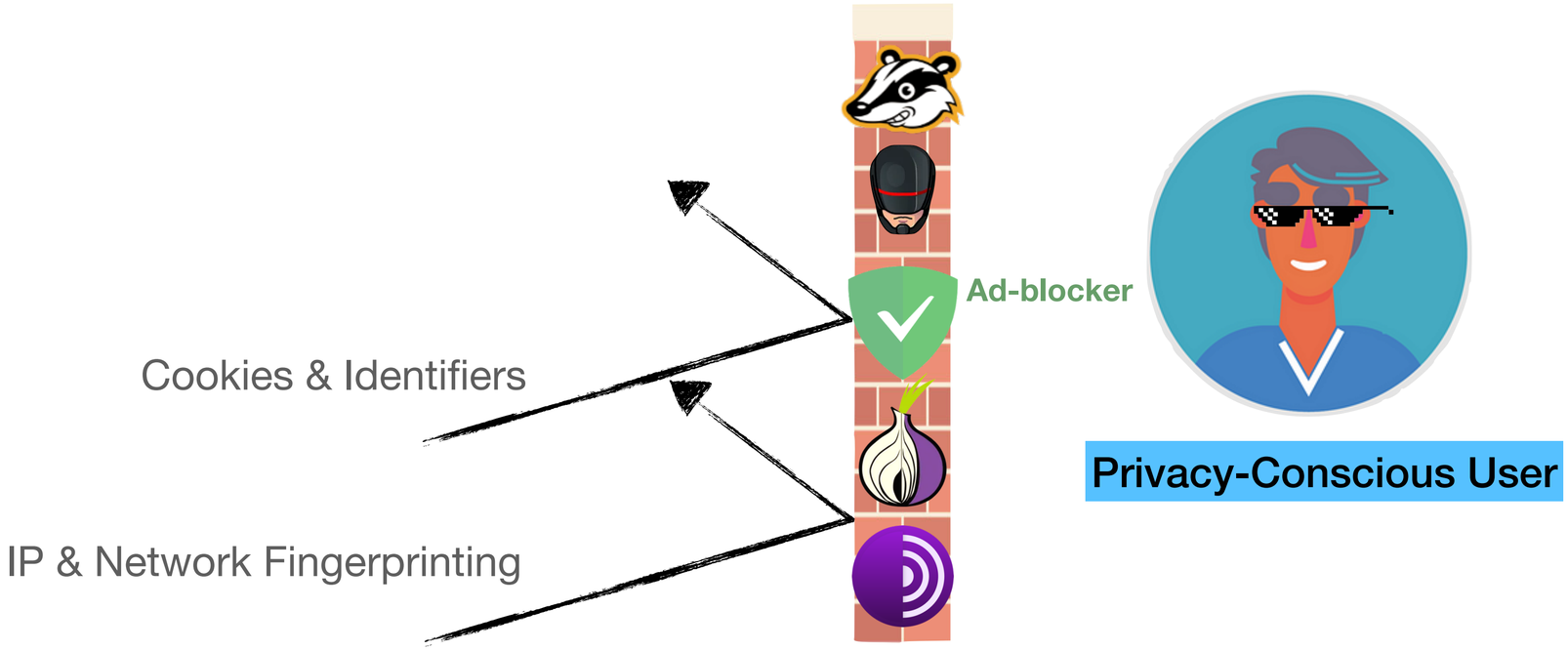


More private ?

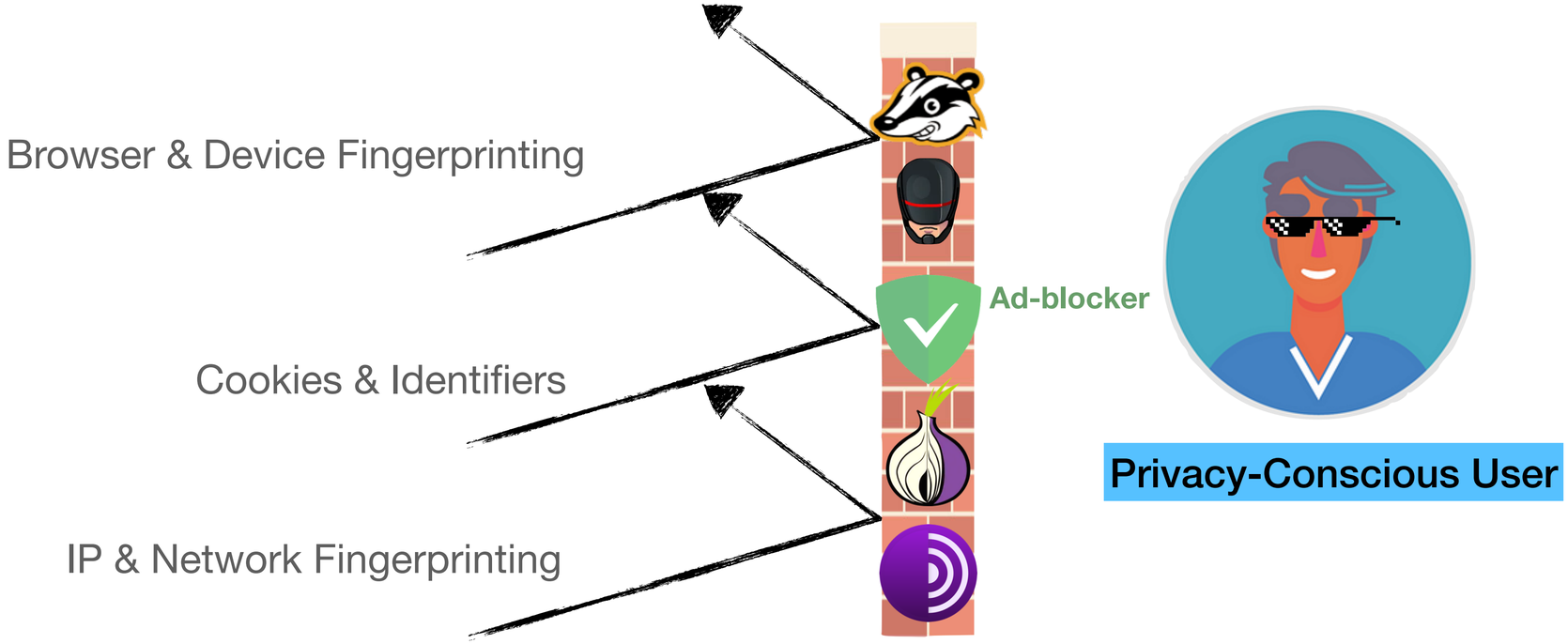
Problem Statement



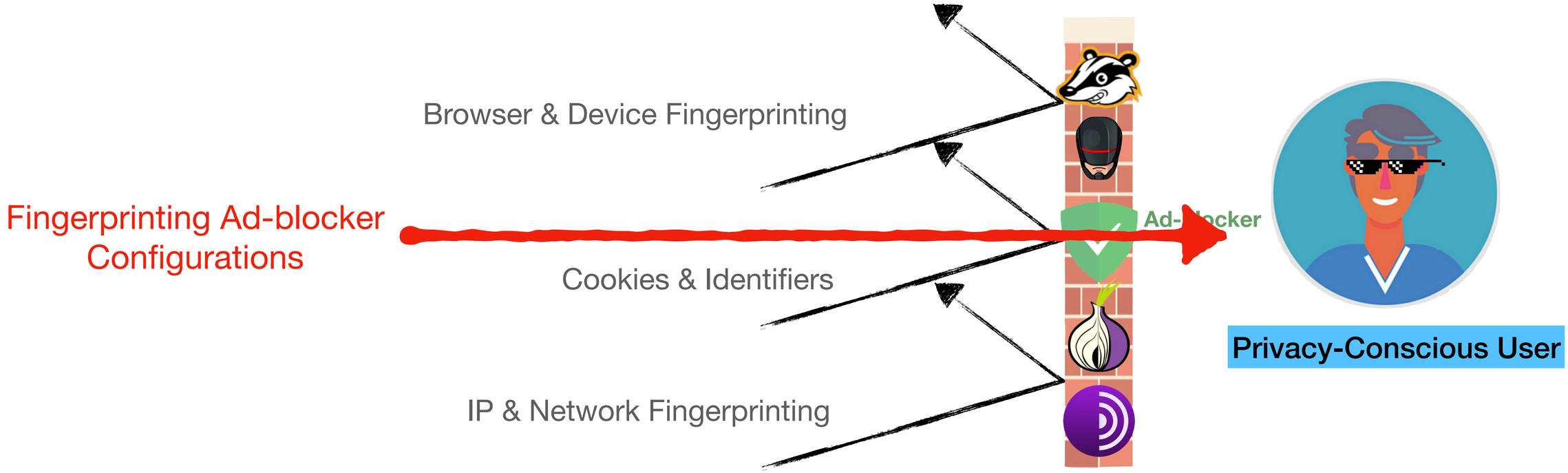
Problem Statement



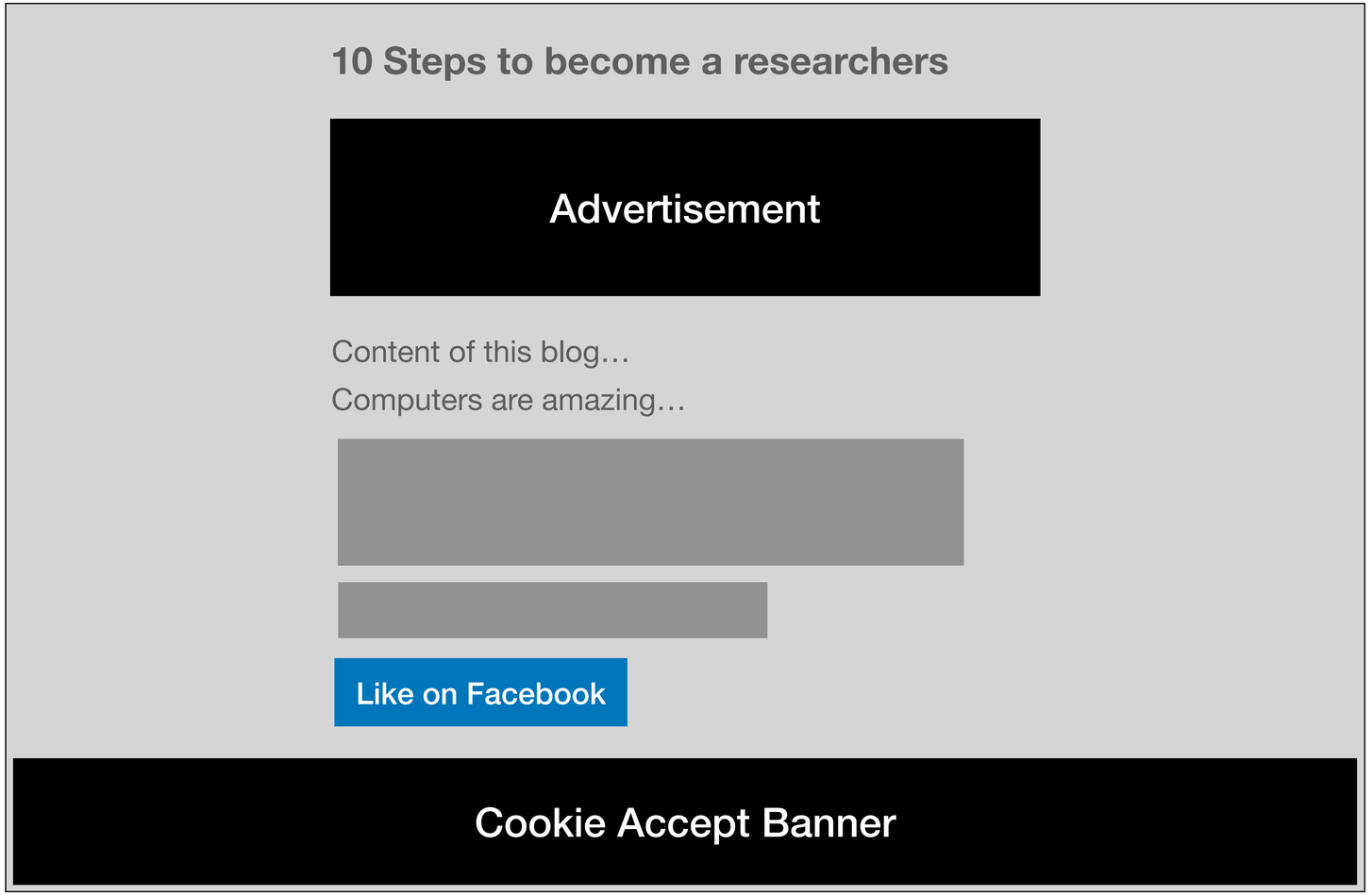
Problem Statement



Problem Statement



How to configure Ad-Blocker



General Ad Blocking

Social Media Buttons

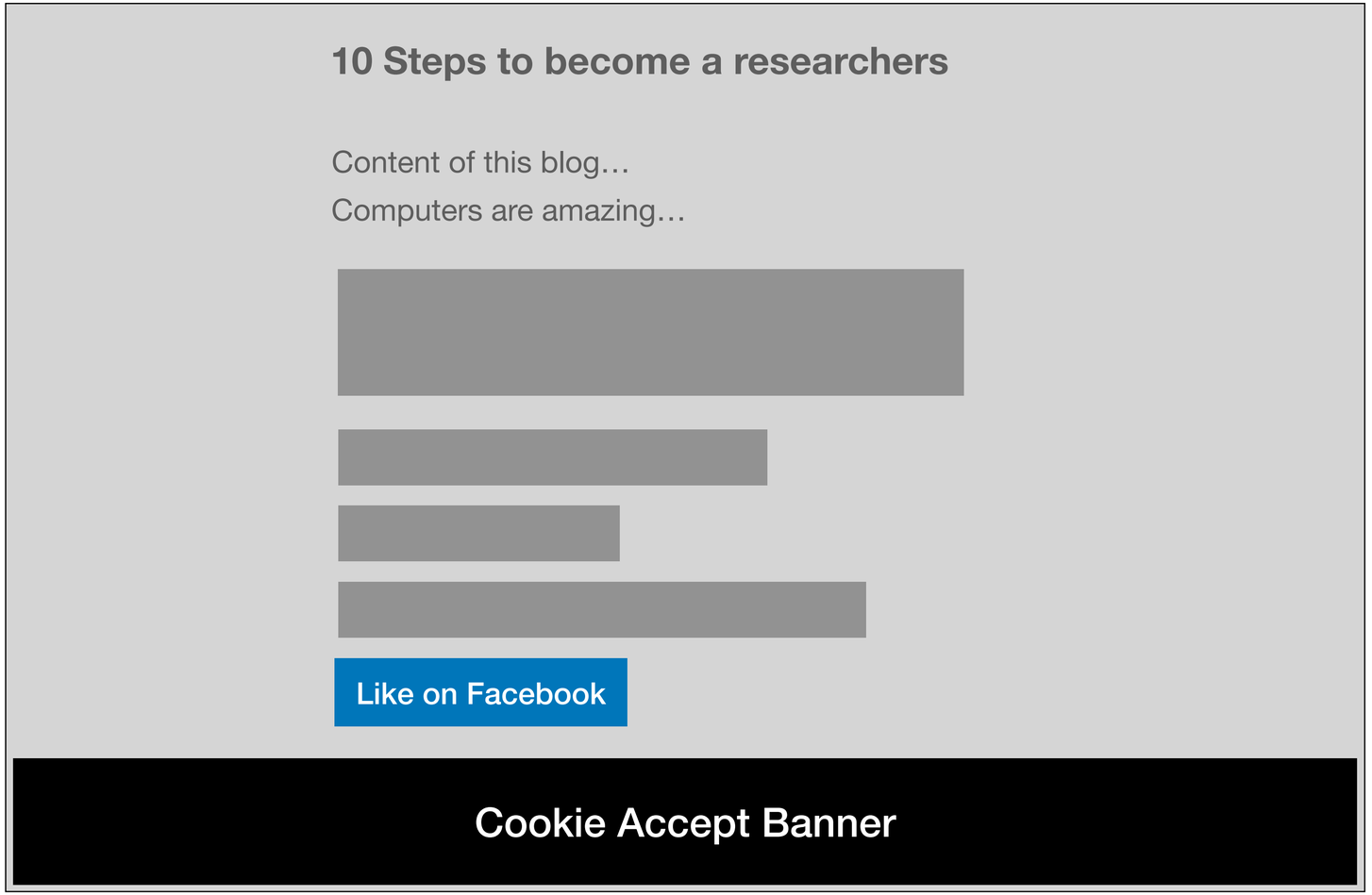
Cookies & Annoyances

Fingerprinting Protections

...

Privacy-Conscious User

How to configure Ad-Blocker



General Ad Blocking

Social Media Buttons

Cookies & Annoyances

Fingerprinting Protections

...

Privacy-Conscious User

How to configure Ad-Blocker

General Ad Blocking

Social Media Buttons

Cookies & Annoyances

Fingerprinting Protections

…

Privacy-Conscious User

Questions we will answer

Can we quantify the privacy harm for “privacy-conscious” users?

Questions we will answer

Can we quantify the privacy harm for “privacy-conscious” users?

1. How is this different than prior fingerprinting attacks?

Questions we will answer

Can we quantify the privacy harm for “privacy-conscious” users?

1. How is this different than prior fingerprinting attacks?
2. Can a malicious website fingerprint this configuration?

Questions we will answer

Can we quantify the privacy harm for “privacy-conscious” users?

1. How is this different than prior fingerprinting attacks?
2. Can a malicious website fingerprint this configuration?
3. How good is this fingerprint in reducing user anonymity?

1. How is this different than prior fingerprinting attacks?

N-Bit Leakage per Extension

1. How is this different than prior fingerprinting attacks?

N-Bit Leakage per Extension

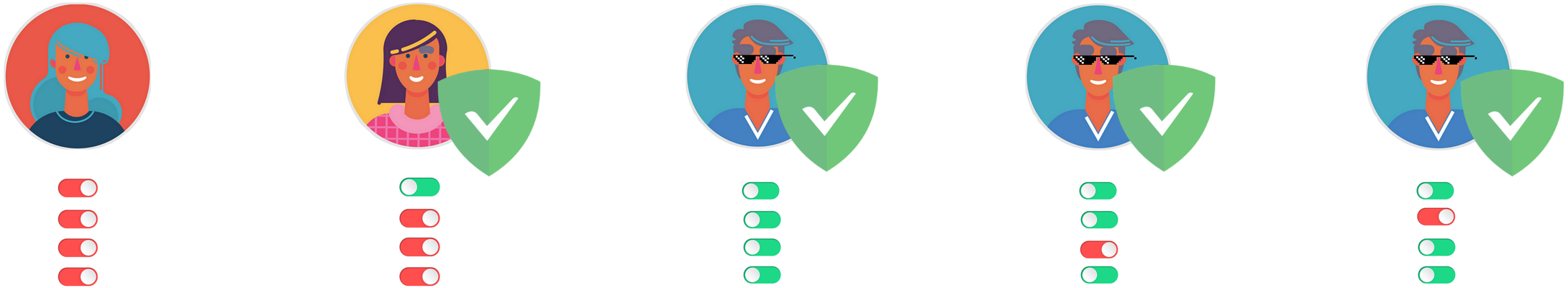




Literature					
Extension	F0	F1	F1	F1	F1
Fingerprinting					

1. How is this different than prior fingerprinting attacks?

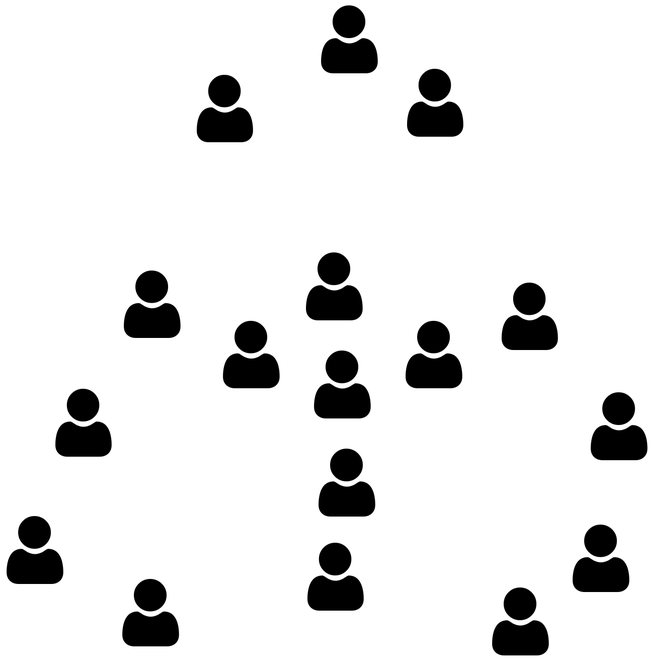
N-Bit Leakage per Extension



Literature Extension Fingerprinting	F0	F1	F1	F1	F1
Our Work	F0000	F1000	F1111	F1101	F1011

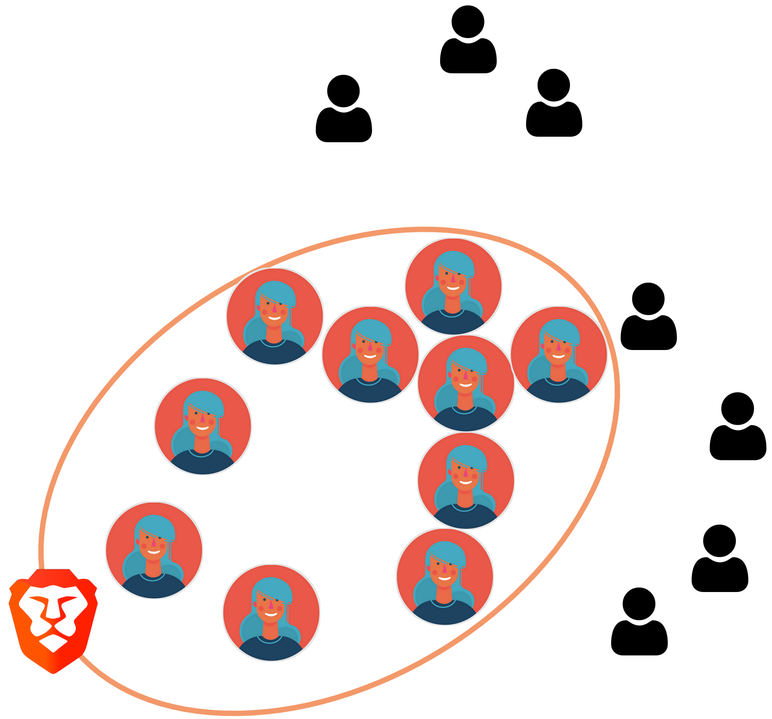
1. How is this different than prior fingerprinting attacks?

Target Users



1. How is this different than prior fingerprinting attacks?

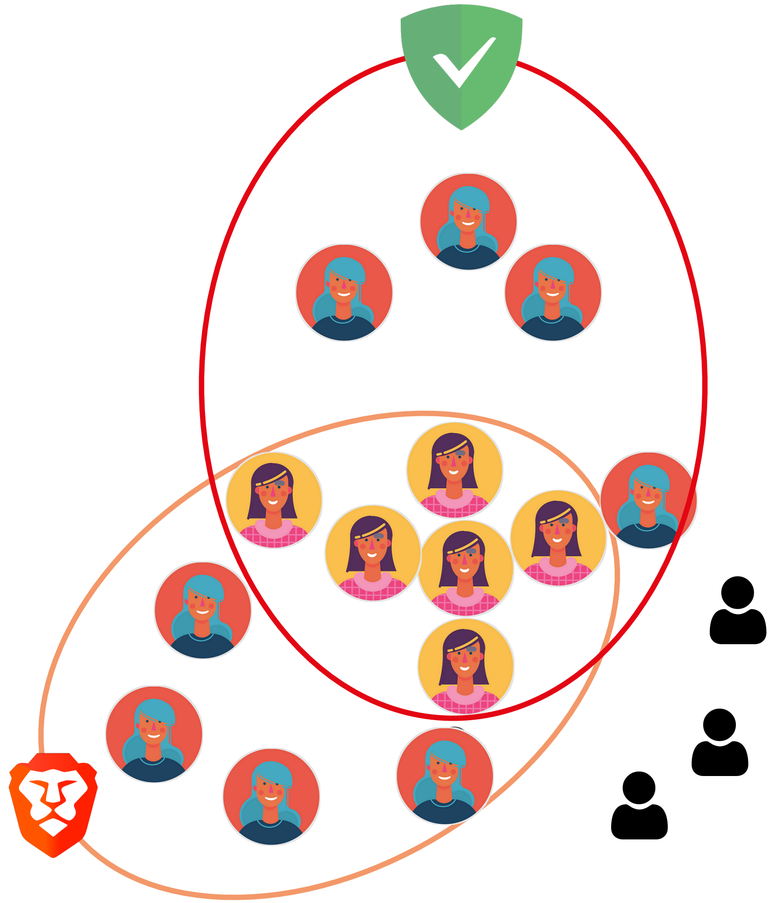
Target Users



Basic User

1. How is this different than prior fingerprinting attacks?

Target Users

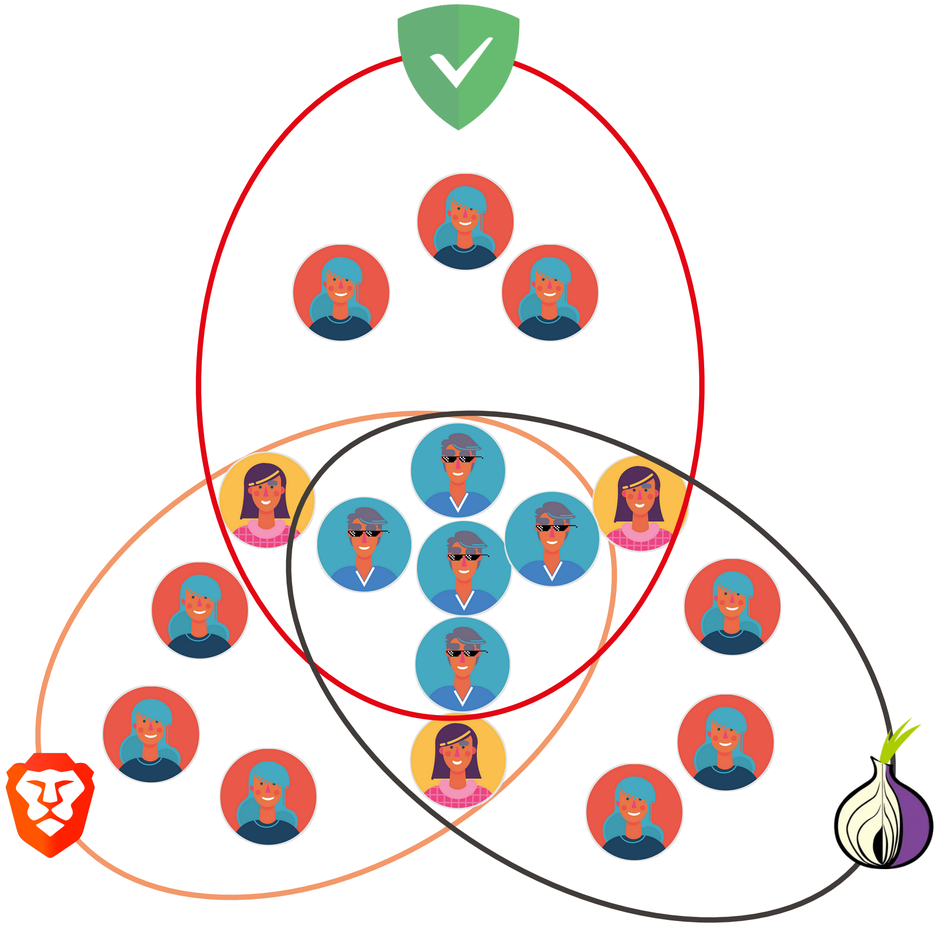



Basic User


More Privacy Concerned

1. How is this different than prior fingerprinting attacks?

Target Users



Basic User

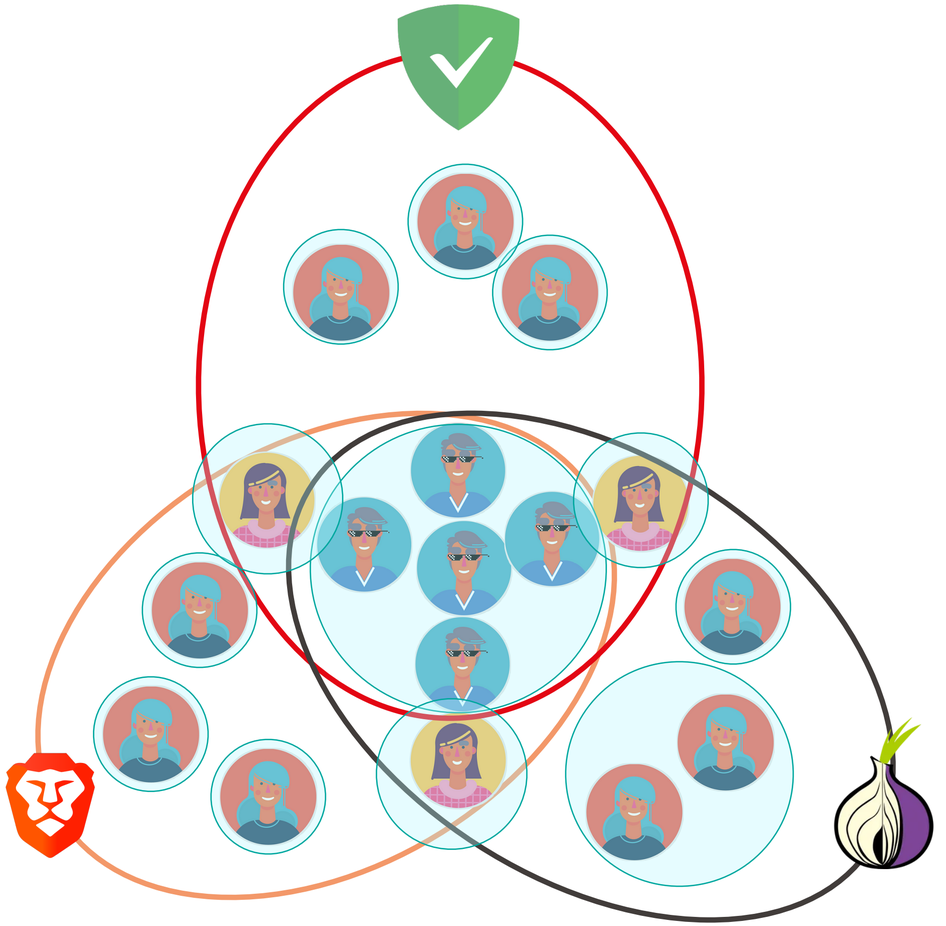
More Privacy Concerned

Privacy Conscious Users

1. How is this different than prior fingerprinting attacks?

Target Users

Prior Studies



Anonymity set

Set of users having the same fingerprint value

Basic User

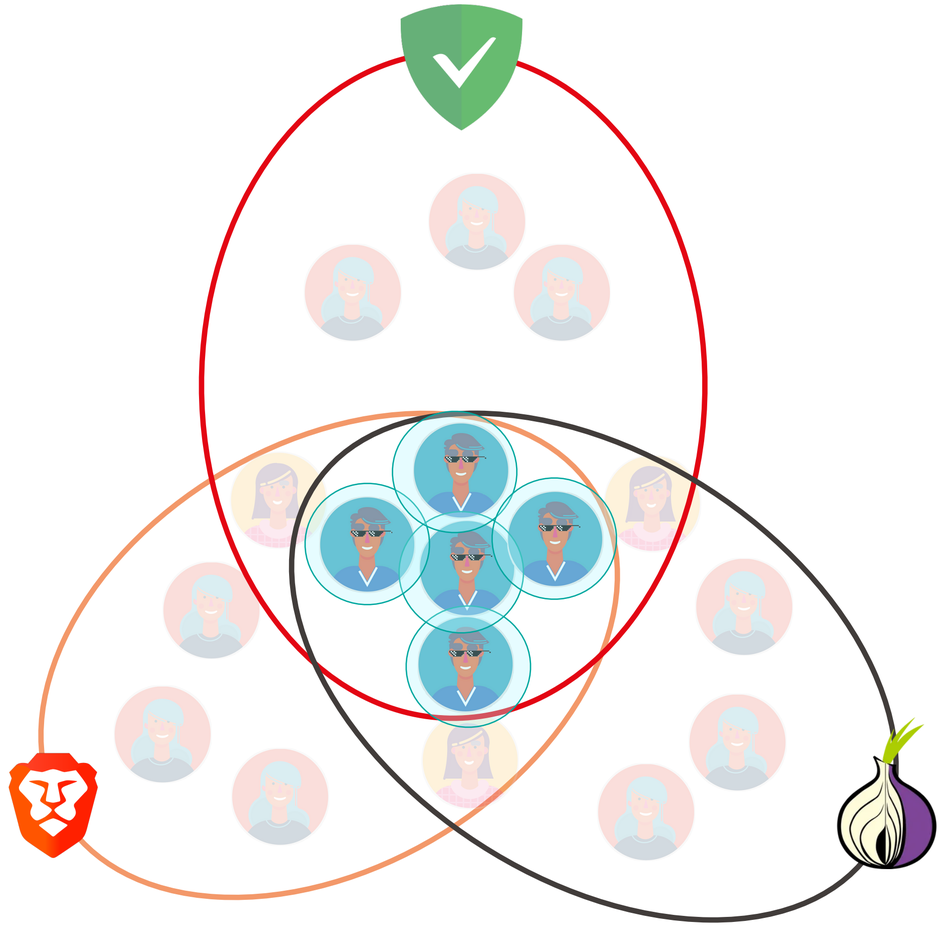
More Privacy Concerned

Privacy Conscious Users

1. How is this different than prior fingerprinting attacks?

Target Users

Our Study



Anonymity set

Set of users having the same fingerprint value

Basic User

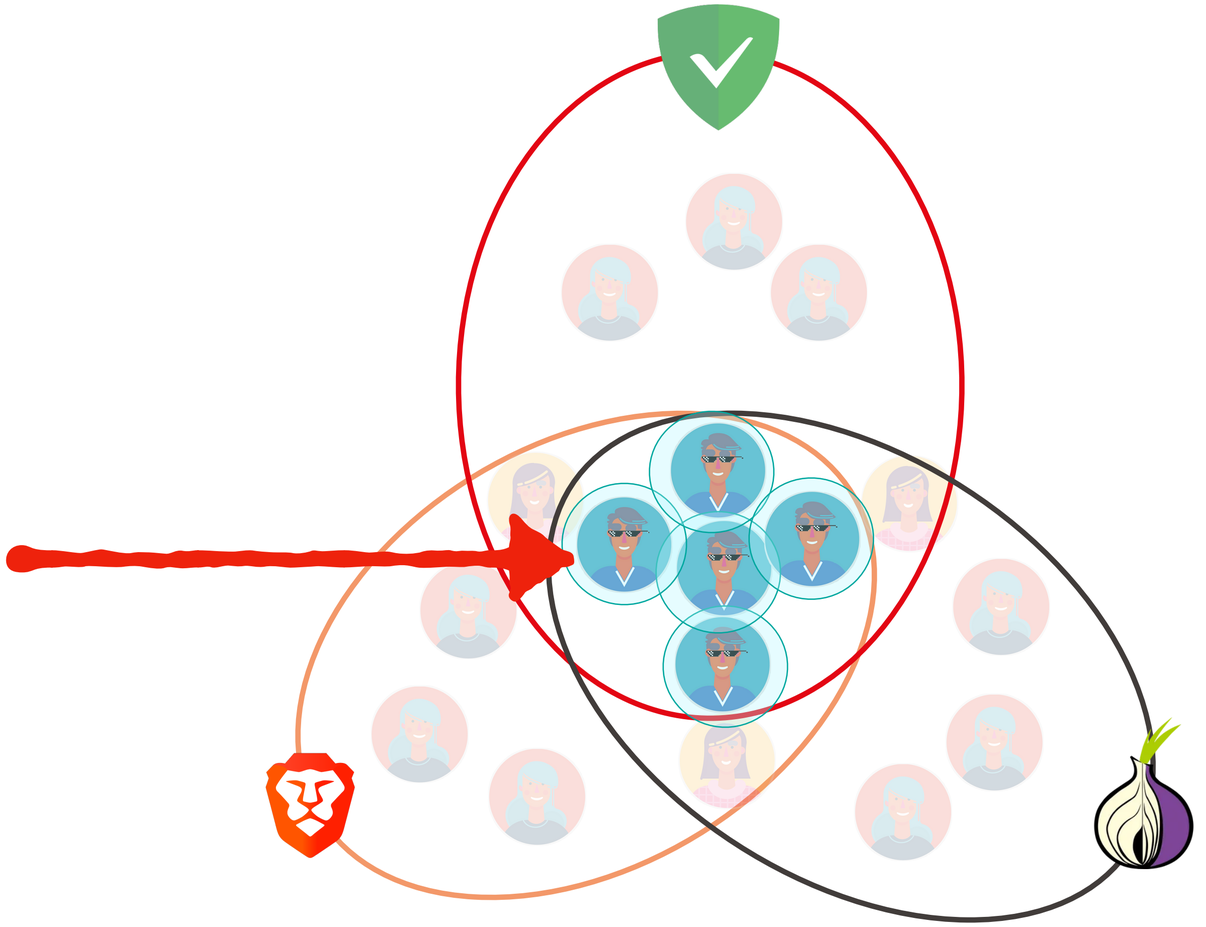
More Privacy Concerned

Privacy Conscious Users

1. How is this different than prior fingerprinting attacks?

Target Users

Our Study



Anonymity set

Set of users having the same fingerprint value

Basic User

More Privacy Concerned

Privacy Conscious Users

2. Can a malicious website fingerprint this configuration?

For Each Config

2. Can a malicious website fingerprint this configuration?

For Each Config

Filter Rules

Block Network Request for Images in ads.de
Hide Cookie Banner #banner-1
...

2. Can a malicious website fingerprint this configuration?

For Each Config

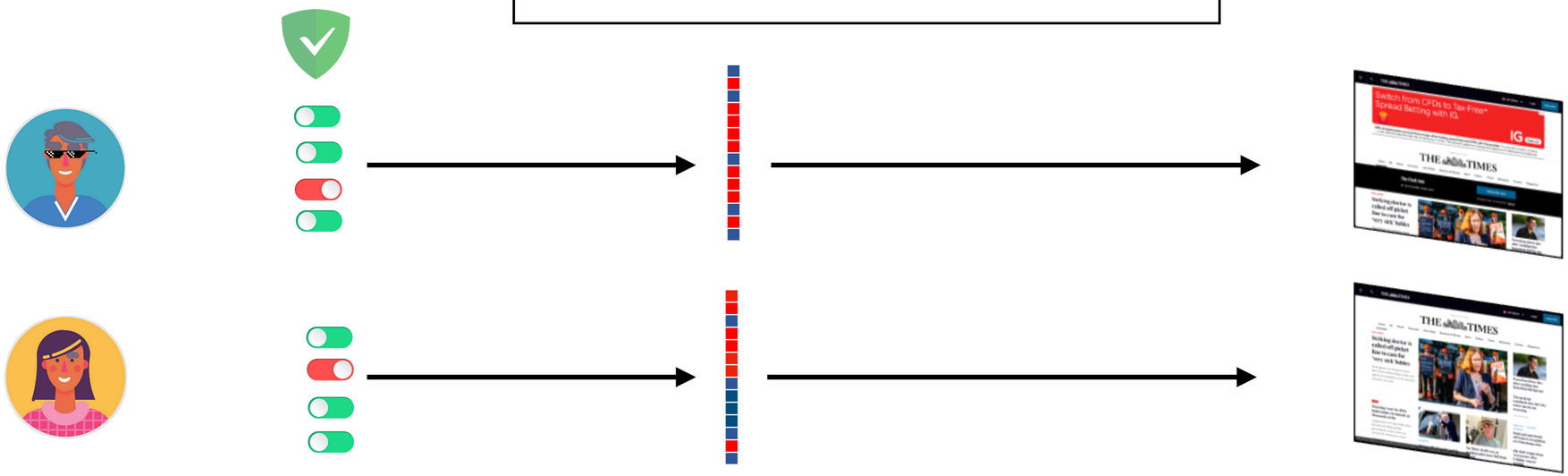
Block German Ads

Filter Rules

Block Network Request for Images in ads.de
Hide Cookie Banner #banner-1
...

Impact on Web Page

Blocking	HTTP Request Blocked
Cosmetic	HTML Element Hidden



2. Can a malicious website fingerprint this configuration?

For Each Config

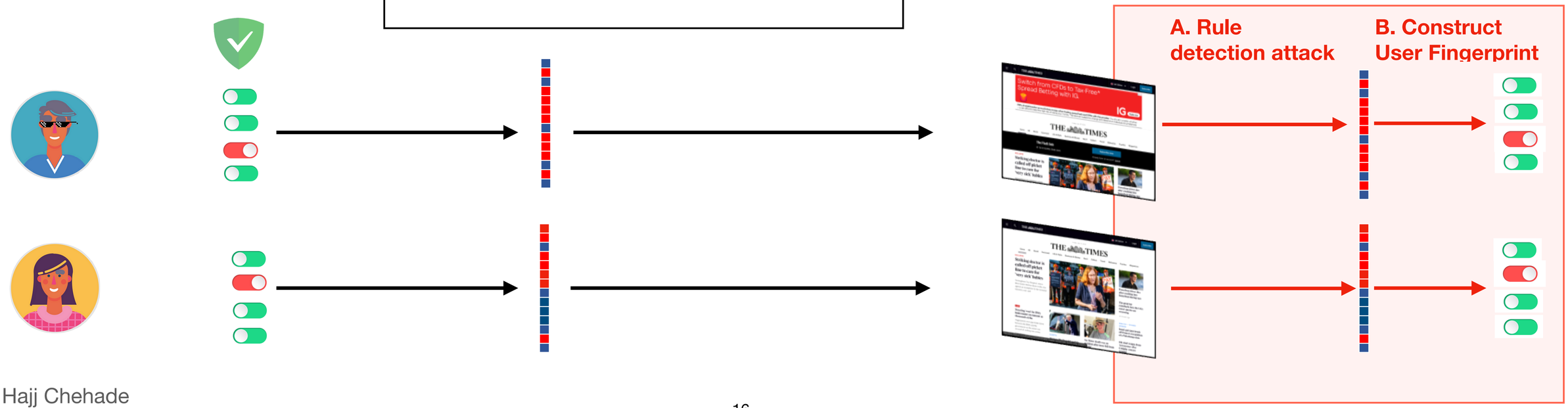
Block German Ads

Filter Rules

Block Network Request for Images in ads.de
Hide Cookie Banner #banner-1
...

Impact on Web Page

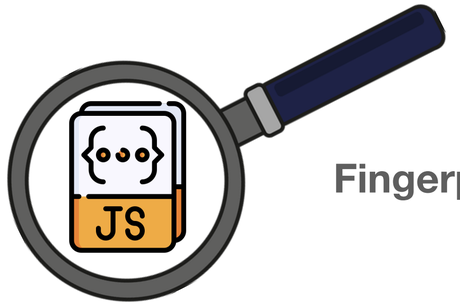
Blocking	HTTP Request Blocked
Cosmetic	HTML Element Hidden



2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

e.g, window.innerWidth



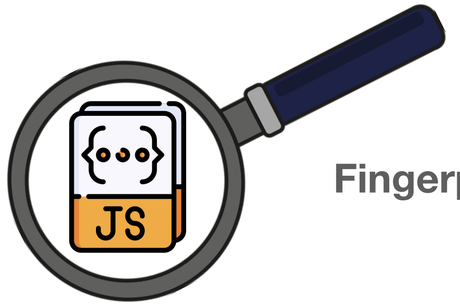
Fingerprinting Detector

!!! Our attacks must overcome state-of-the-art fingerprinting detectors

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

e.g, window.innerWidth



Fingerprinting Detector

!!! Our attacks must overcome state-of-the-art fingerprinting detectors

No JavaScript => Stylistic (CSS-based) Fingerprinting

Example:

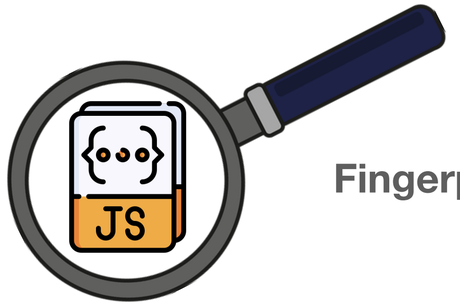
```
@media (min-width: 300px) {
  #probe {background: url(/iframe-width-300);}}
@media (min-width: 301px) {
  #probe {background: url(/iframe-width-301);}}
...
@media (min-width: 600px) {
  #probe {background: url(/iframe-width-600);}}
```

Lin, Xu, et al. "Fashion Faux Pas: Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses." IEEE S&P, 2023.

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

e.g, window.innerWidth



Fingerprinting Detector

!!! Our attacks must overcome state-of-the-art fingerprinting detectors

No JavaScript => Stylistic (CSS-based) Fingerprinting

Fewest possible requests => fewest signals

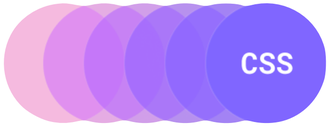
Example:

```
@media (min-width: 300px) {
  #probe {background: url(/iframe-width-300);}}
@media (min-width: 301px) {
  #probe {background: url(/iframe-width-301);}}
...
@media (min-width: 600px) {
  #probe {background: url(/iframe-width-600);}}
```

Lin, Xu, et al. "Fashion Faux Pas: Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses." IEEE S&P, 2023.

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks



CSS Animation Attack

Intuition

Evaluating styles only on visible elements leaks visibility.

Image Lazy Loading Attack

Intuition

Browser optimization of loading images almost visible leaks height of elements above them.

```
@container (width > 15em){
  /* stylesheet */
}
```

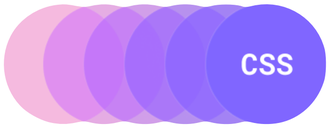
`@container` Query Attack

Intuition Experimental

Executing styles contingent on other element **computed** styles leaks information about element alterations.

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks



CSS Animation Attack

Intuition

Evaluating styles only on visible elements leaks visibility.

Image Lazy Loading Attack

Intuition

Browser optimization of loading images almost visible leaks height of elements above them.

```
@container (width > 15em){
  /* stylesheet */
}
```

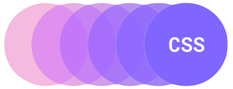
`@container` Query Attack

Intuition Experimental

Executing styles contingent on other element **computed** styles leaks information about element alterations.

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks



CSS Animation Attack

Attack HTML and CSS

```
<img id="detector-1"
src="blocked.com/im.png"/>
```

```
#detector-1 {
  animation: my-anim 1s;
}
@keyframes anim {
100% {
  background-image: attacker.com/signals/123;
}
}
```

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

CSS Animation Attack

Rule active:

Attack HTML and CSS

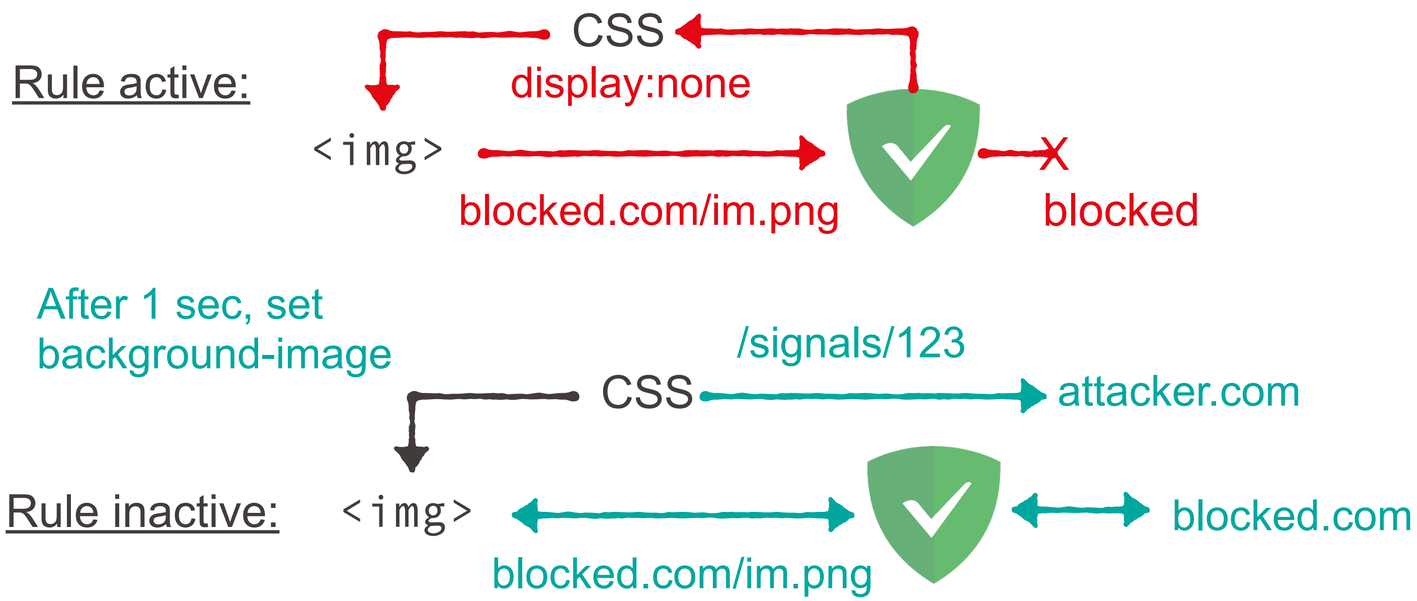
```
<img id="detector-1"
src="blocked.com/im.png"/>
```

```
#detector-1 {
  animation: my-anim 1s;
}
@keyframes anim {
100% {
  background-image: attacker.com/signals/123;
}
}
```

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

CSS Animation Attack



Attack HTML and CSS

```
<img id="detector-1"
src="blocked.com/im.png"/>
```

```
#detector-1 {
  animation: my-anim 1s;
}
@keyframes anim {
100% {
  background-image: attacker.com/signals/123;
}
}
```

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

CSS Animation Attack

Intuition

Evaluating styles only on visible elements leaks visibility.

Image Lazy Loading Attack

Intuition

Browser optimization of loading images almost visible leaks height of elements above them.

```
@container (width > 15em){
  /* stylesheet */
}
```

`@container` Query Attack

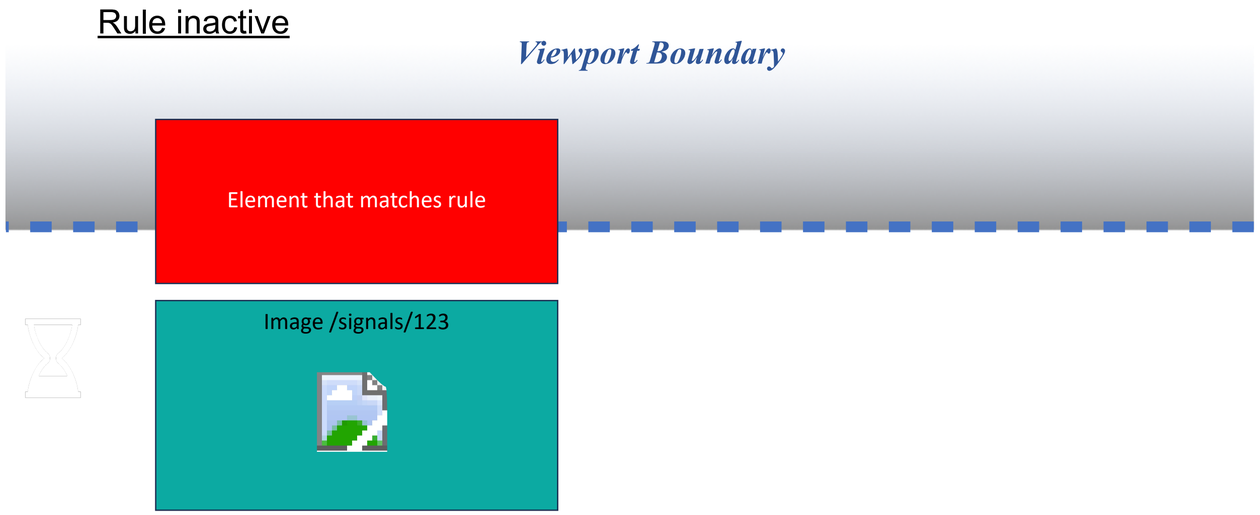
Intuition Experimental

Executing styles contingent on other element **computed** styles leaks information about element alterations.

2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

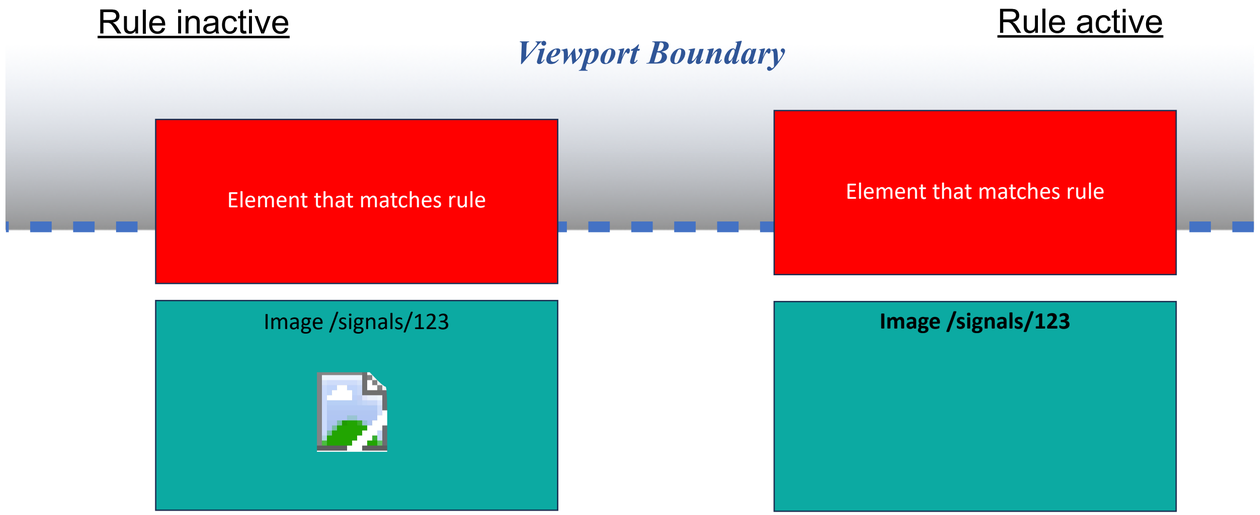
Image Lazy Loading Attack



2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

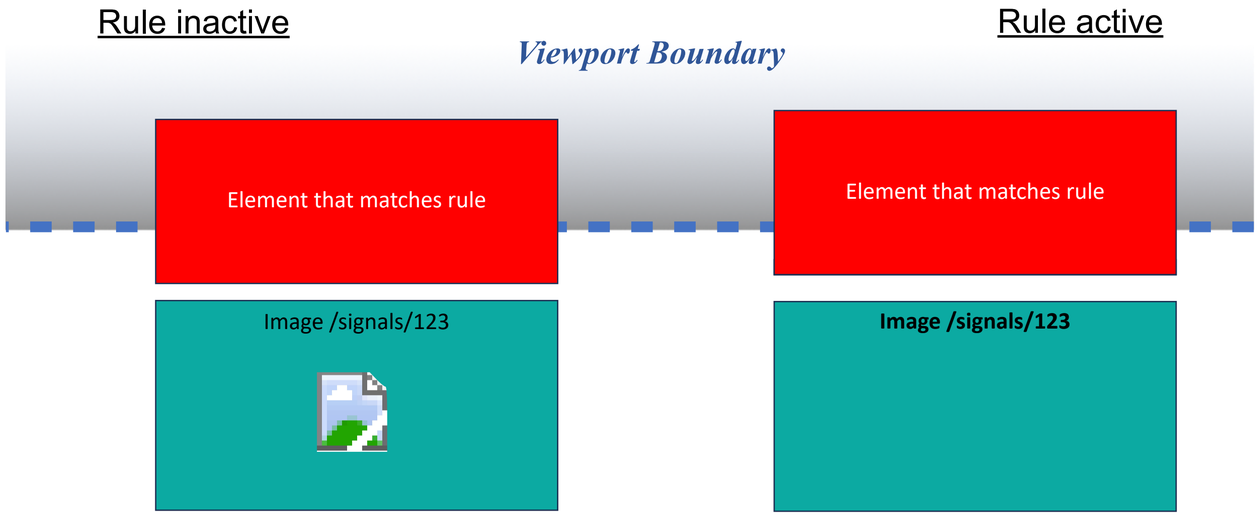
Image Lazy Loading Attack



2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

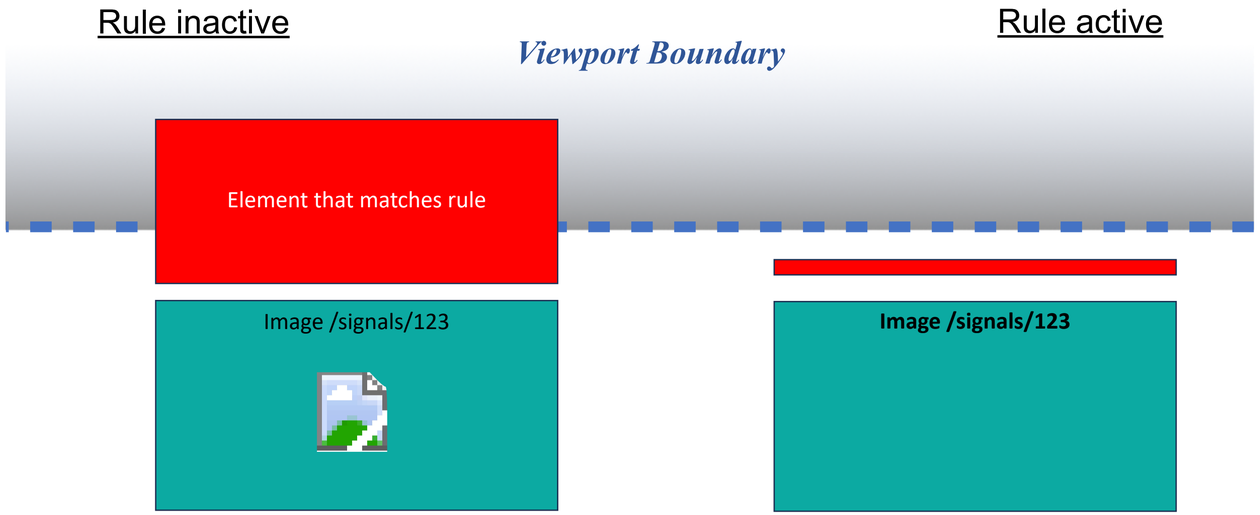
Image Lazy Loading Attack



2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

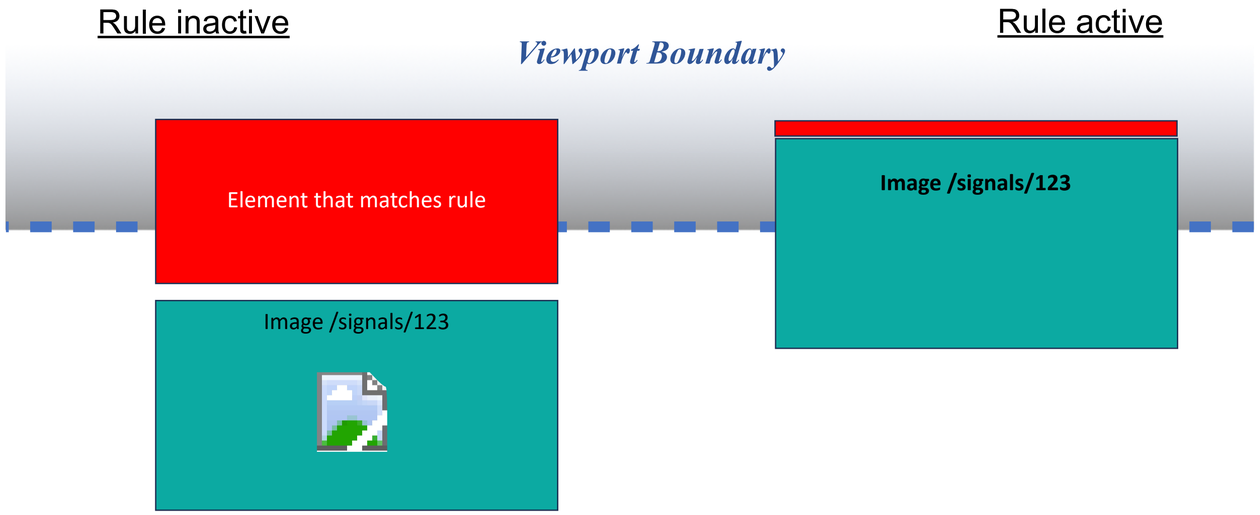
Image Lazy Loading Attack



2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

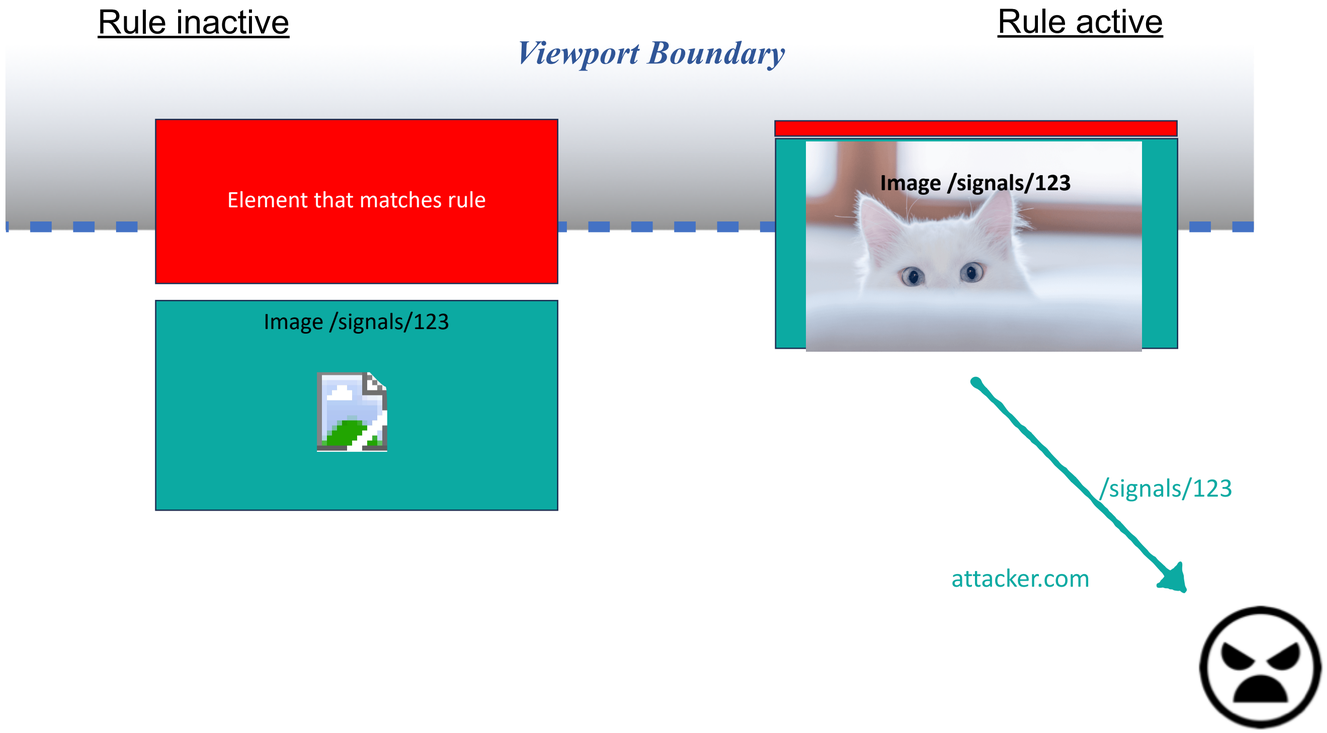
Image Lazy Loading Attack



2. Can a malicious website fingerprint this configuration?

A. Rule detection attacks

Image Lazy Loading Attack



2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

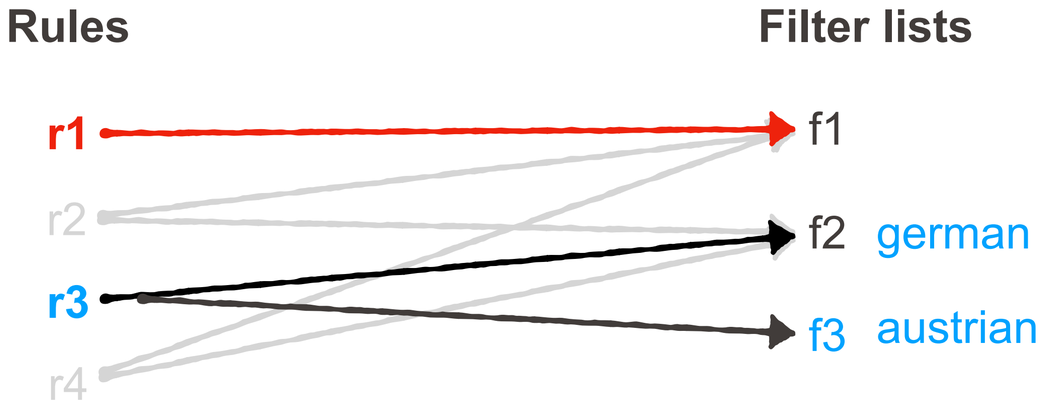
1. Users configure ad-blockers at the **filter-list** granularity → Maximize detectable **filter-lists**

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

1. Users configure ad-blockers at the **filter-list** granularity → Maximize detectable **filter-lists**
2. **Filter-lists** could have shared rules

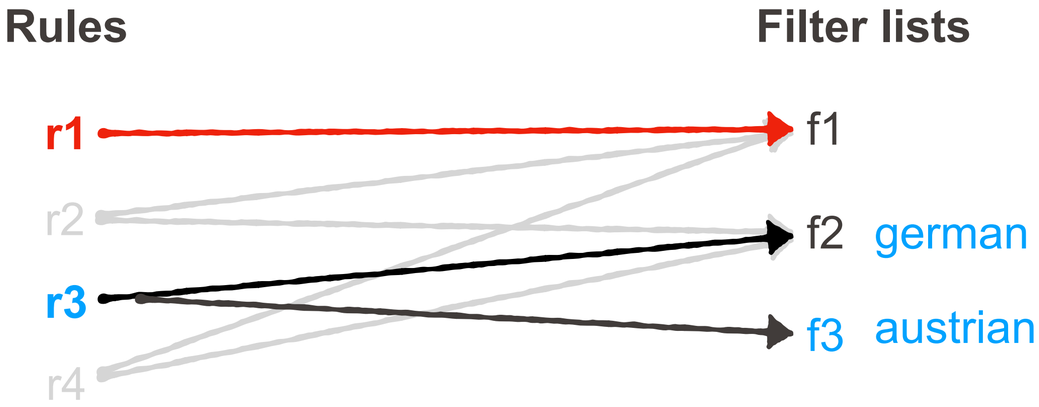


2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

1. Users configure ad-blockers at the **filter-list** granularity → Maximize detectable **filter-lists**
2. **Filter-lists** could have shared rules



Equivalence Sets

e1: {r1} ⇔ {f1}

e2: {r2, r4} ⇔ {f1, f2}

e2: {r3} ⇔ {f2, f3}

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

Test **some** rules

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

More than 400 equivalences? Least number of rules for maximum harm

Test **some** rules → Infer **some** configuration knobs  → Most Unique User Fingerprint [1, 0, 1]

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

More than 400 equivalences? Least number of rules for maximum harm

Test **some** rules → Infer **some** configuration knobs → Most Unique User Fingerprint [1, 0, 1]

Targeted Fingerprint

*Best **m** tests to minimize the anonymity set size of target user **U***

G. G. Gulyas et al. Near-Optimal Fingerprinting with Constraints. In PETS, 2016

2. Can a malicious website fingerprint this configuration?

B. Constructing User Fingerprint

More than 100K rules? Find smallest set of useful rules to identify most configuration knobs

More than 400 equivalences? Least number of rules for maximum harm

Test **some** rules → Infer **some** configuration knobs  → Most Unique User Fingerprint [1, 0, 1]

Targeted Fingerprint

*Best **m** tests to minimize the anonymity set size of target user **U***

General Fingerprint

*Best **m** tests to minimize the **average anonymity set size** (or maximize Shannon entropy).*

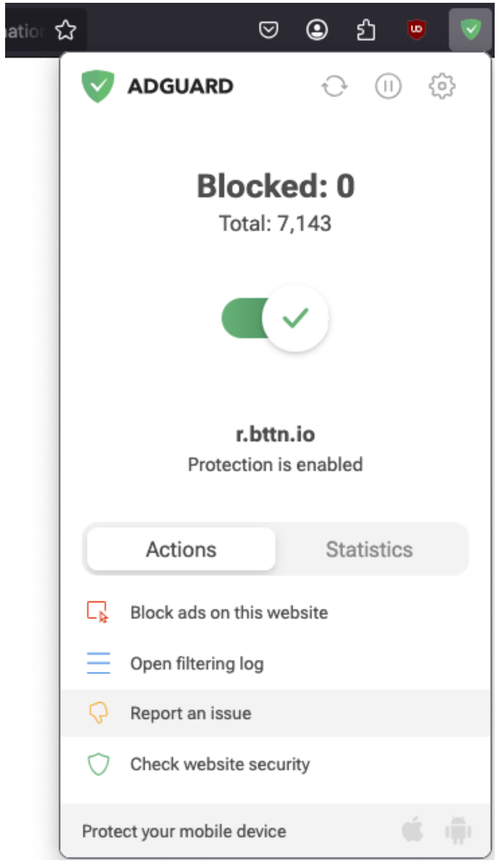
G. G. Gulyas et al. Near-Optimal Fingerprinting with Constraints. In PETS, 2016

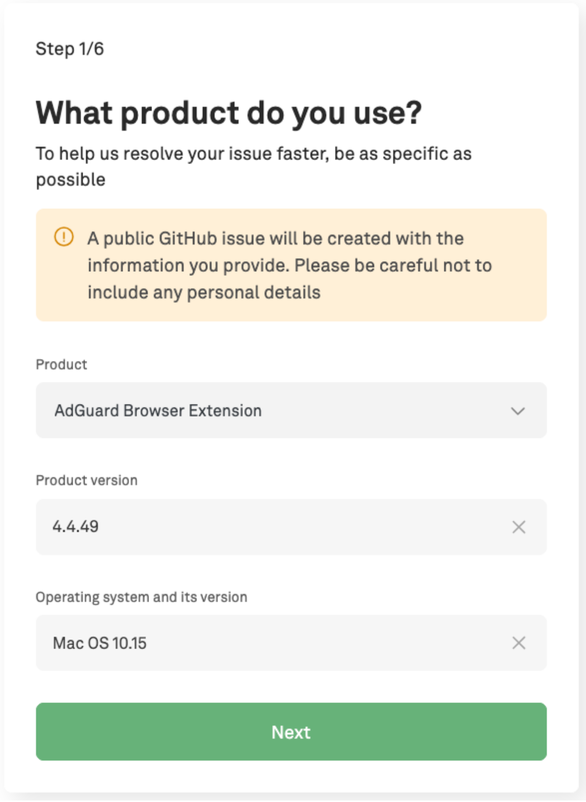
3. How good is this fingerprint in reducing user anonymity?

3. How good is this fingerprint in reducing user anonymity?

Evaluation

Datasets > GitHub Issues

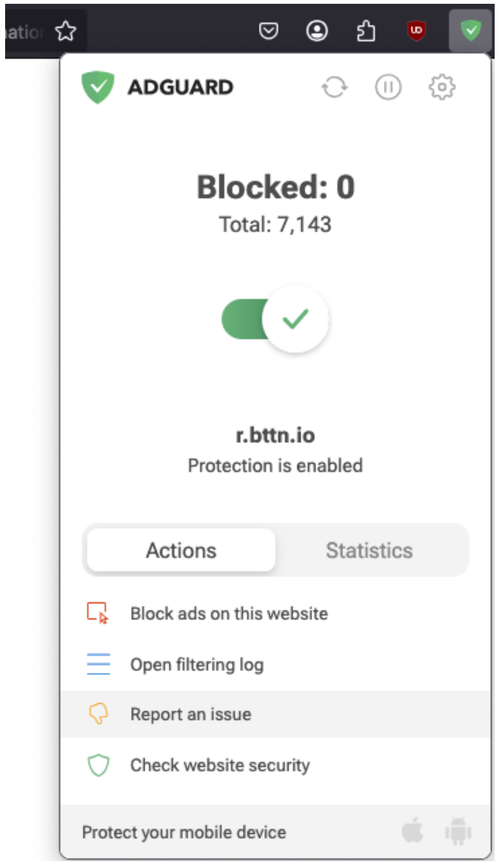


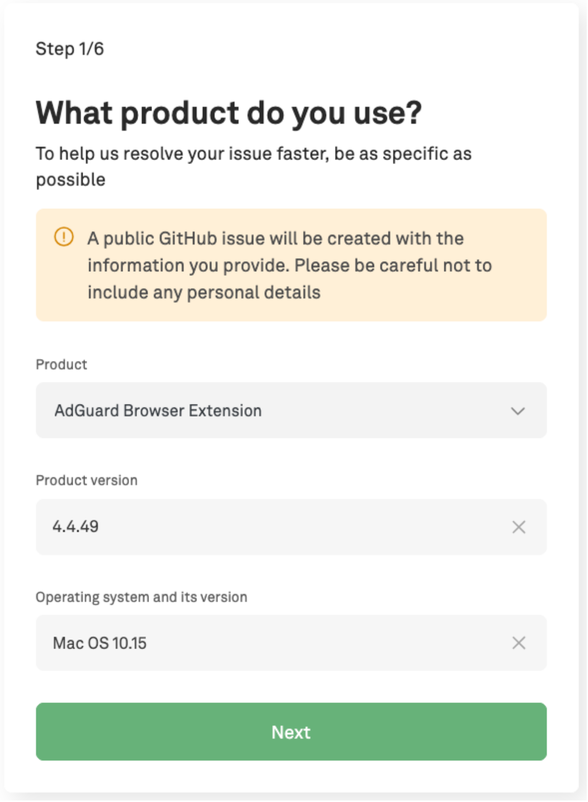


3. How good is this fingerprint in reducing user ar

Evaluation

Datasets > GitHub Issues





System configuration

Information	Value
AdGuard product:	AdGuard for Android v4.9
System version:	android15 galaxys23
Browser:	삼성 브라우저
License type:	paid
AdGuard mode:	VPN
HTTPS filtering:	enabled
Tracking protection:	**General settings:** Block trackers, Strip URLs from tracking parameters, Send Do-Not-Track header **Browser API:** Block WebRTC, Block Push API, Block Location API **Miscellaneous:** Remove X-Client-Data header from HTTP requests, Protect against DPI
DNS filtering:	disabled
Filters:	**Ad blocking:** AdGuard Base, AdGuard Mobile Ads **Privacy:** AdGuard Tracking Protection, AdGuard URL Tracking **Annoyances:** AdGuard Annoyances **Language-specific:** AdGuard Japanese, List-KR
Browsing Security:	disabled
Browsing Security statistics:	disabled
Userscripts:	tinyshield Namulink Disable AMP Adguard Extra

3. How good is this fingerprint in reducing user anonymity?

Evaluation

Datasets > Ad-blockers

uBlock Origin

44

Million installs

87

filter lists

AdGuard

15

Million installs

68

filter lists

3. How good is this fingerprint in reducing user anonymity?

Evaluation

Datasets > Ad-blockers

uBlock Origin

44
Million installs

87
filter lists

5.9K
Users

AdGuard

15
Million installs

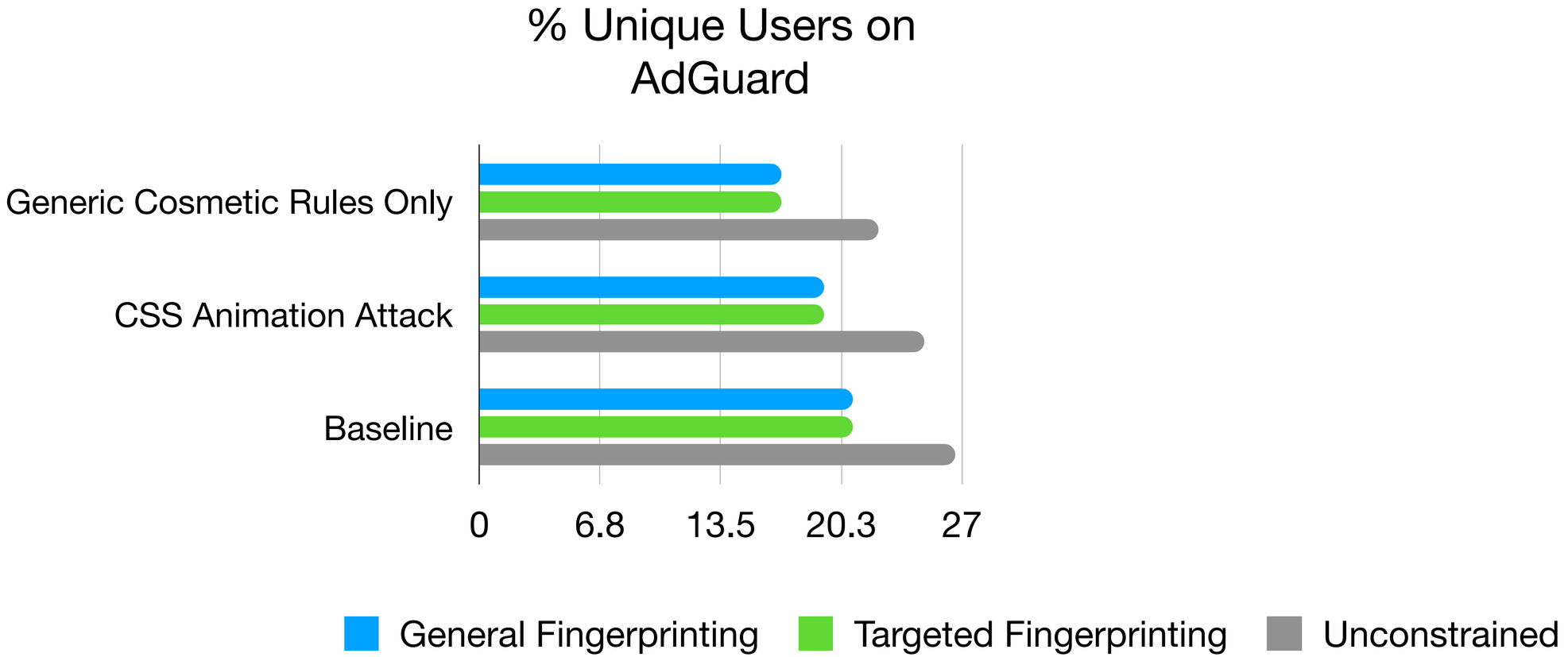
68
filter lists

18.5K
Users

3. How good is this fingerprint in reducing user anonymity?

Evaluation

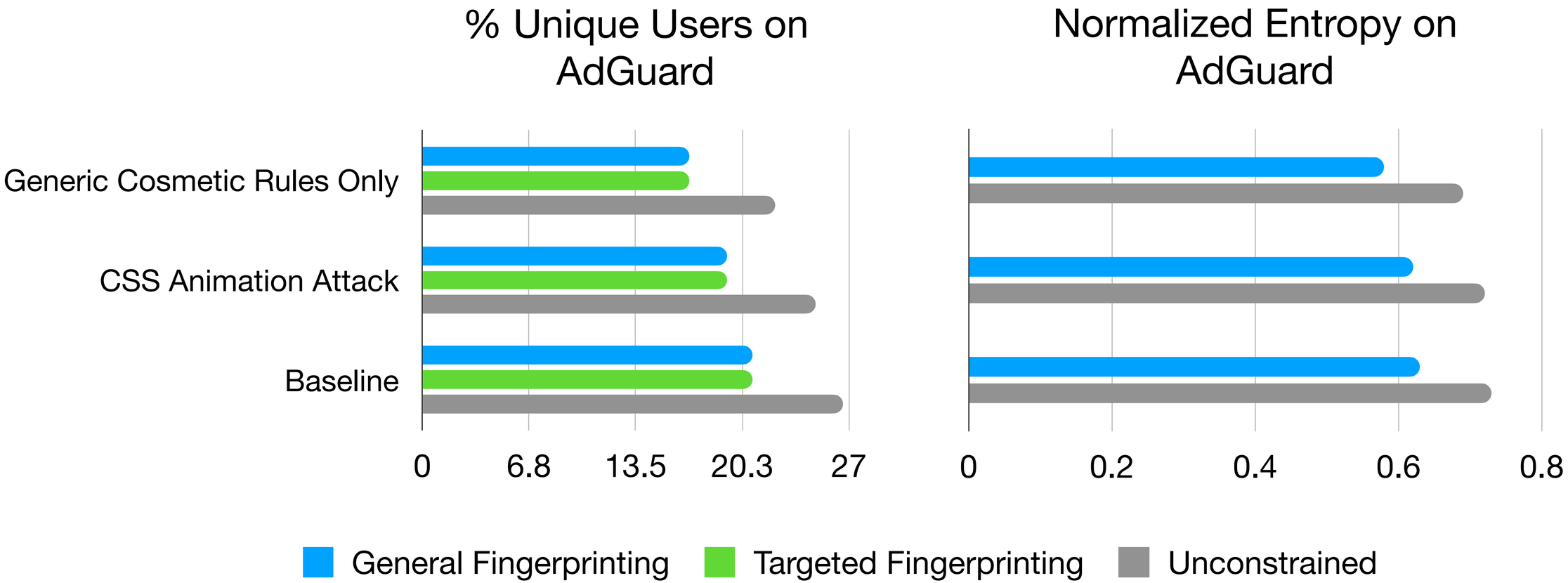
User Anonymity



3. How good is this fingerprint in reducing user anonymity?

Evaluation

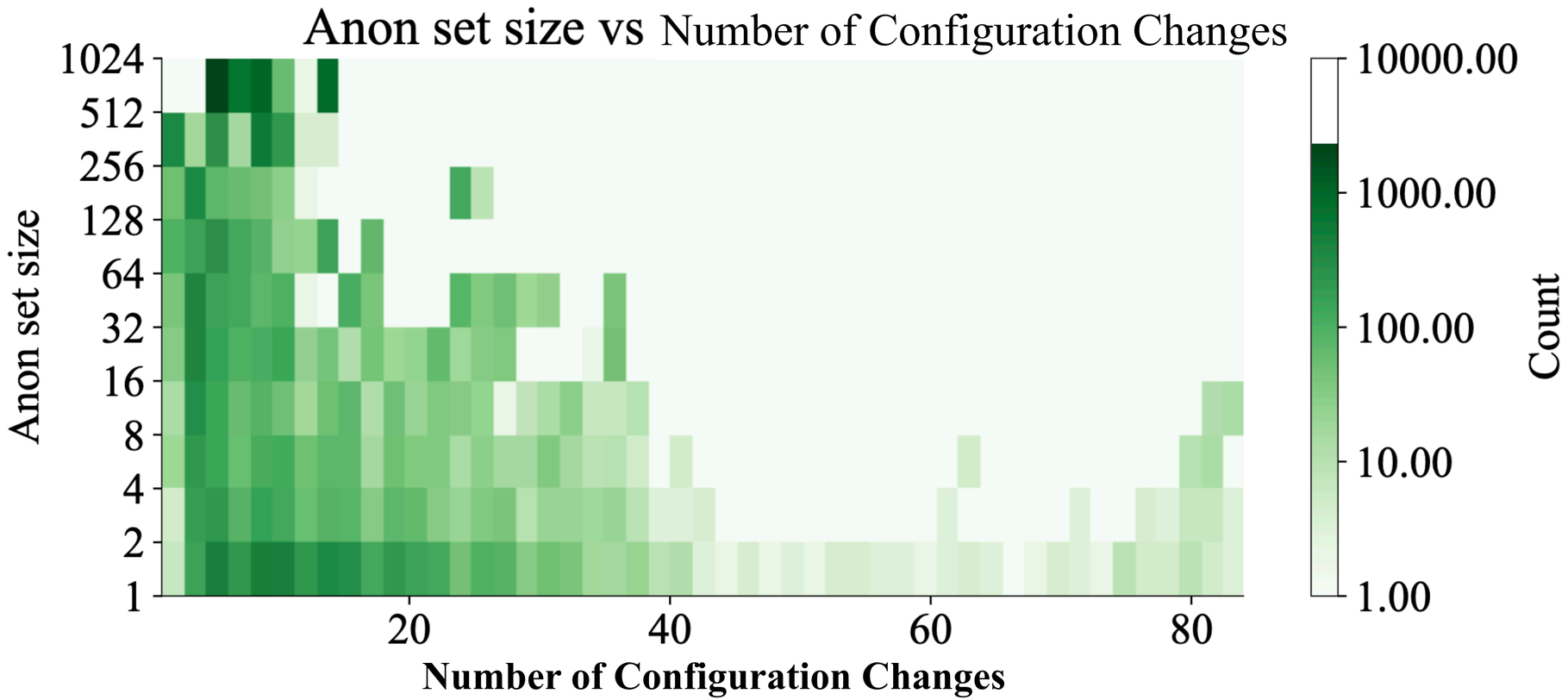
User Anonymity



3. How good is this fingerprint in reducing user anonymity?

Evaluation

User Anonymity

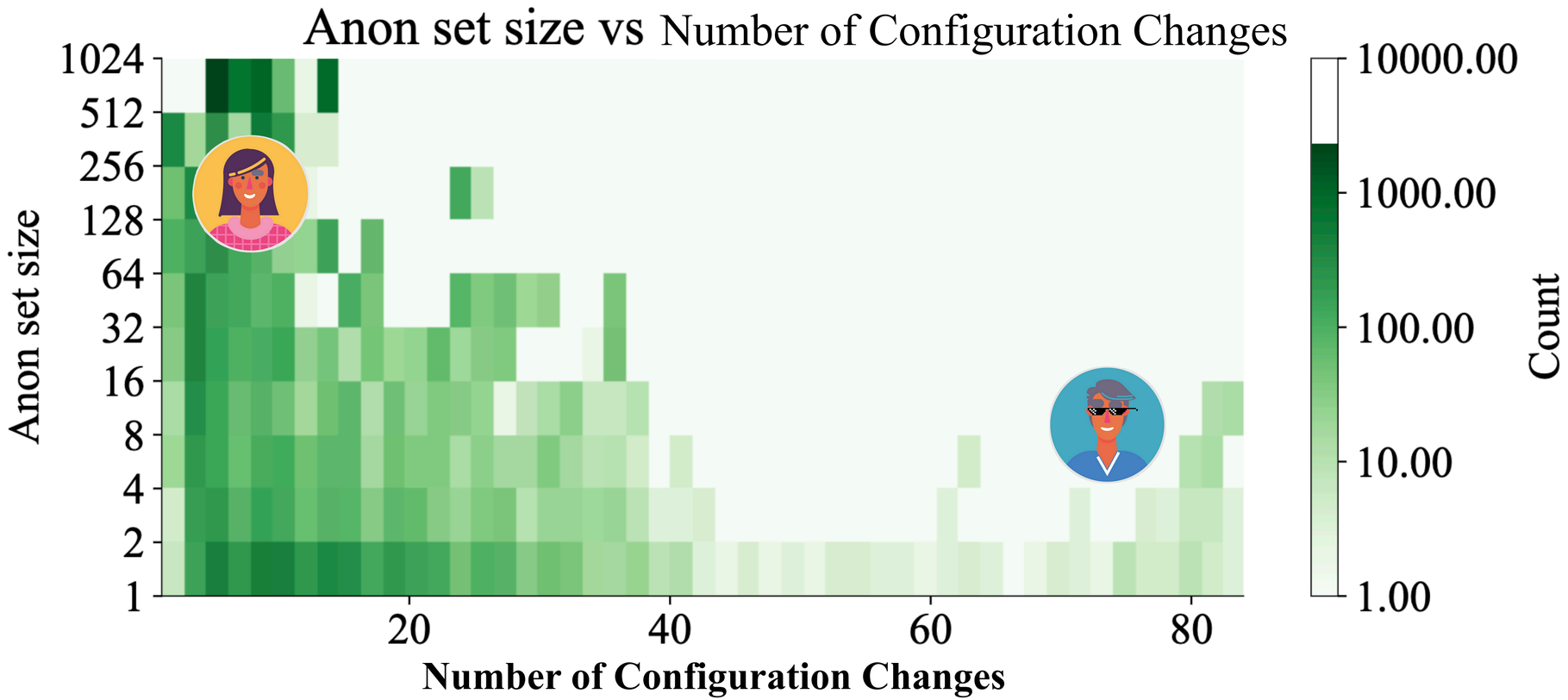


3. How good is this fingerprint in reducing user anonymity?

Evaluation

User Anonymity

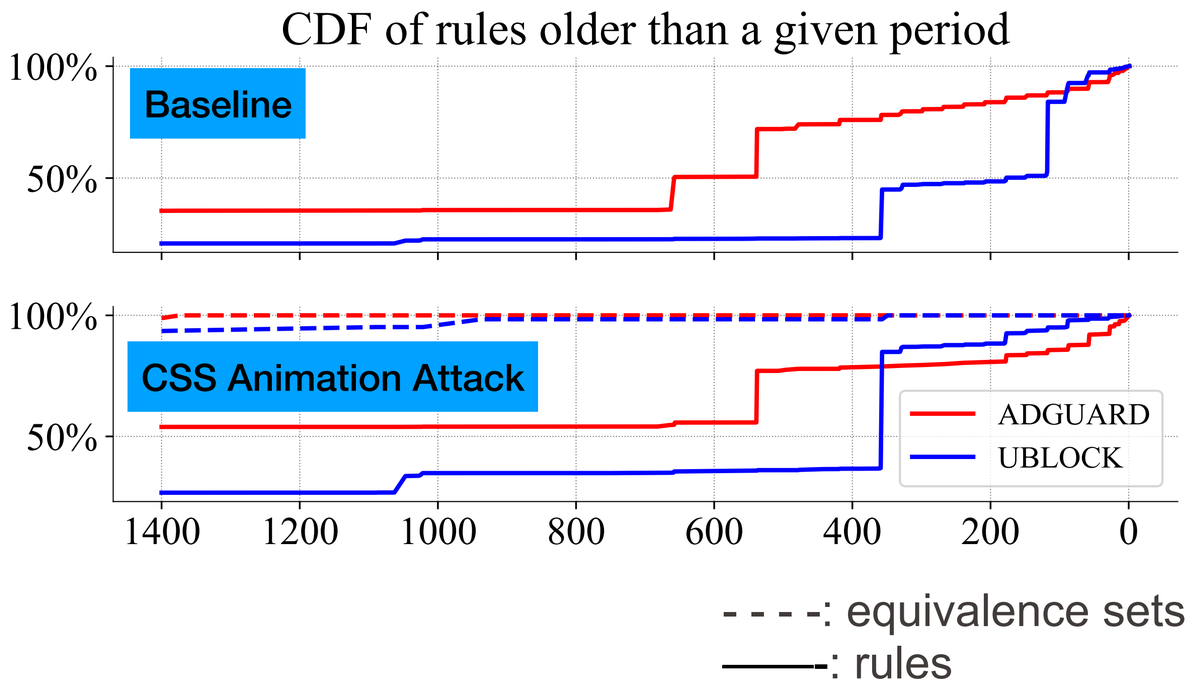
Hypothesis Confirmed! Advanced “Privacy-Conscious” users have smaller anonymity sets



2. How good is this fingerprint in reducing user anonymity?

Evaluation

Filter-list Coverage User Anonymity Fingerprint Stability



Are fingerprints stable against filter-list updates?

At least **3 years** of equivalence set stability

2. How good is this fingerprint in reducing user anonymity?

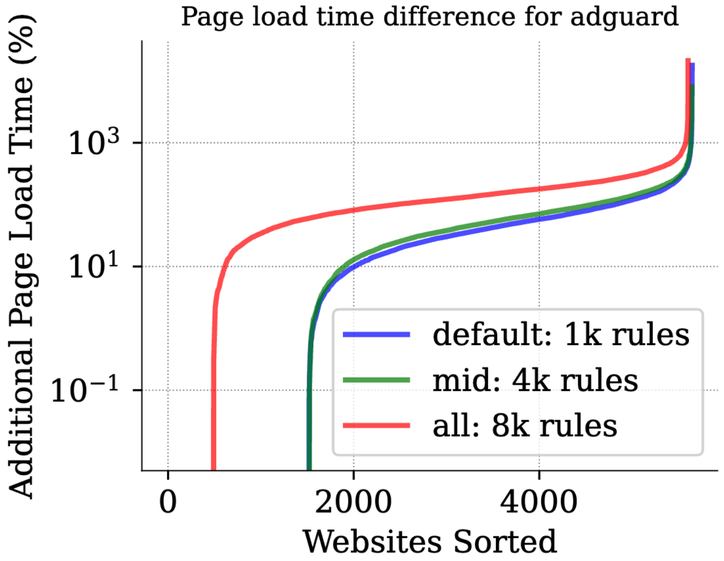
Evaluation

Filter-list Coverage User Anonymity Fingerprint Stability Detection & Mitigation

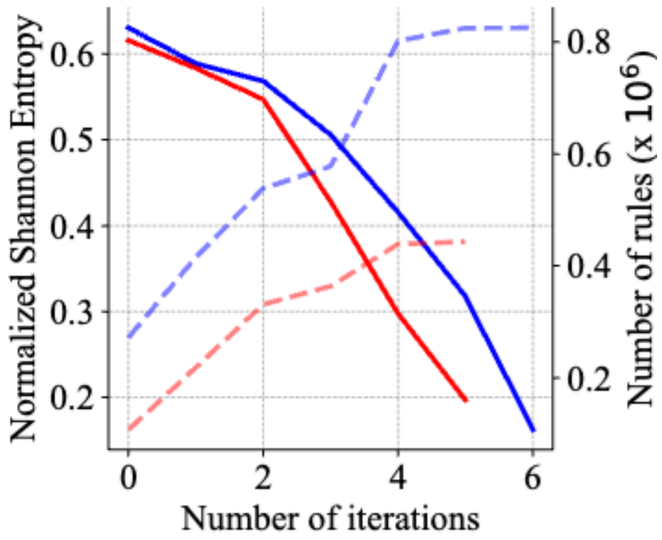
2. How good is this fingerprint in reducing user anonymity?

Evaluation

Filter-list Coverage User Anonymity Fingerprint Stability Detection & Mitigation



Mitigations



Disallow Customization

high performance load

Globally enabling Vulnerable Rules

Promising for uBlock
Might cause breakage

Disabling Browser Features

Needs granular CSS decisions
Might cause breakage

Takeaways

- Users with **advanced** privacy setups are susceptible to **unique fingerprinting risks.**
- Practical **scriptless** attacks that achieve 0.6 entropy similar to prior work.
- We validate fingerprint stability and evaluate mitigation strategies.
- We provide recommendations for maintainers, users, and browsers.

Try the attack on your ad-blocker :)

https://flfp-demo.github.io/

Take a look at the paper!

Contact me

https://saiid.ch

saiid.elhajjchehade@epfl.ch