Fashion Faux Pas

Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses

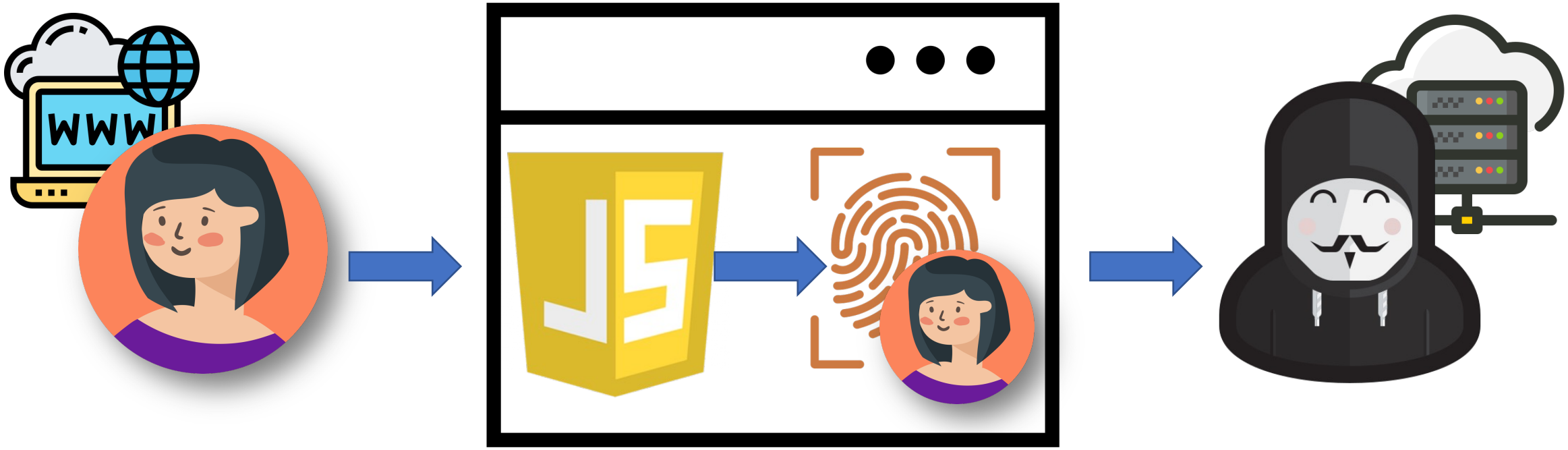
Xu Lin*, Frederico Araujo † , Teryl Taylor †, Jiyong Jang † , Jason Polakis*

* University of Illinois Chicago
† IBM Research

xlin48@uic.edu

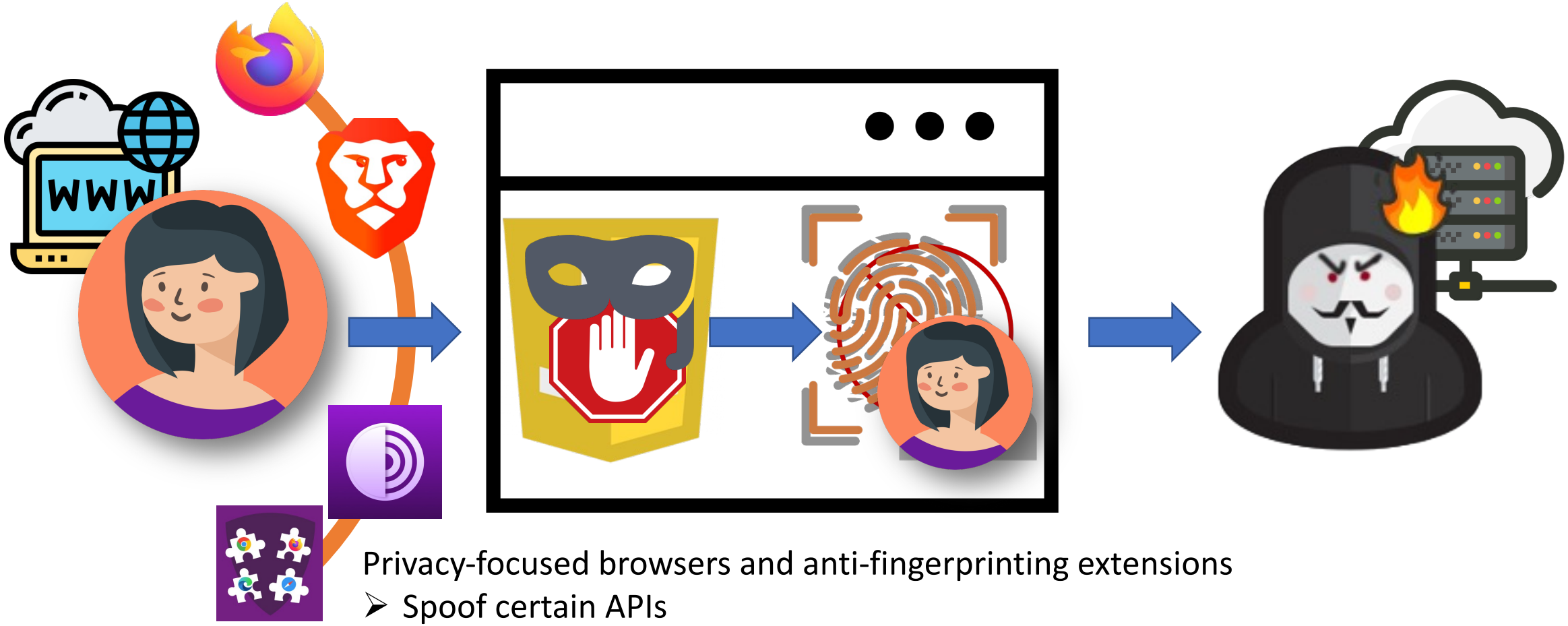
IEEE Symposium on Security and Privacy 2023

Online tracking



Browser fingerprinting heavily relies on JavaScript.

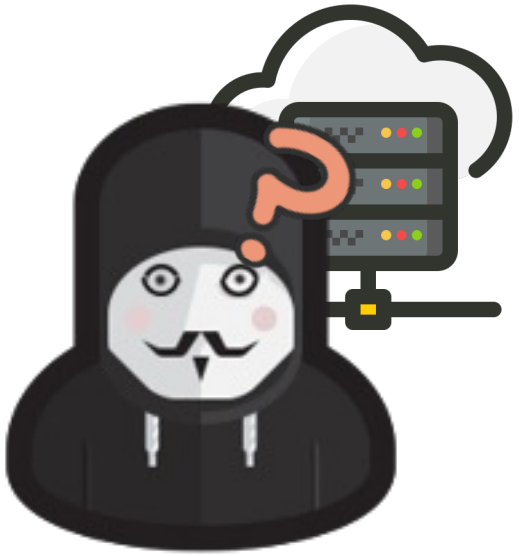
Fingerprinting countermeasures

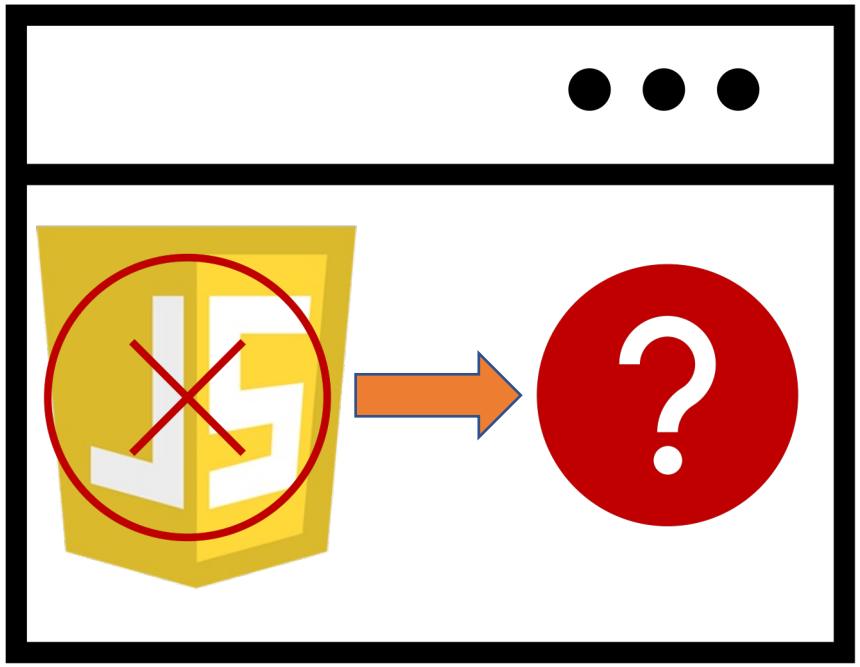


Privacy-focused browsers and anti-fingerprinting extensions

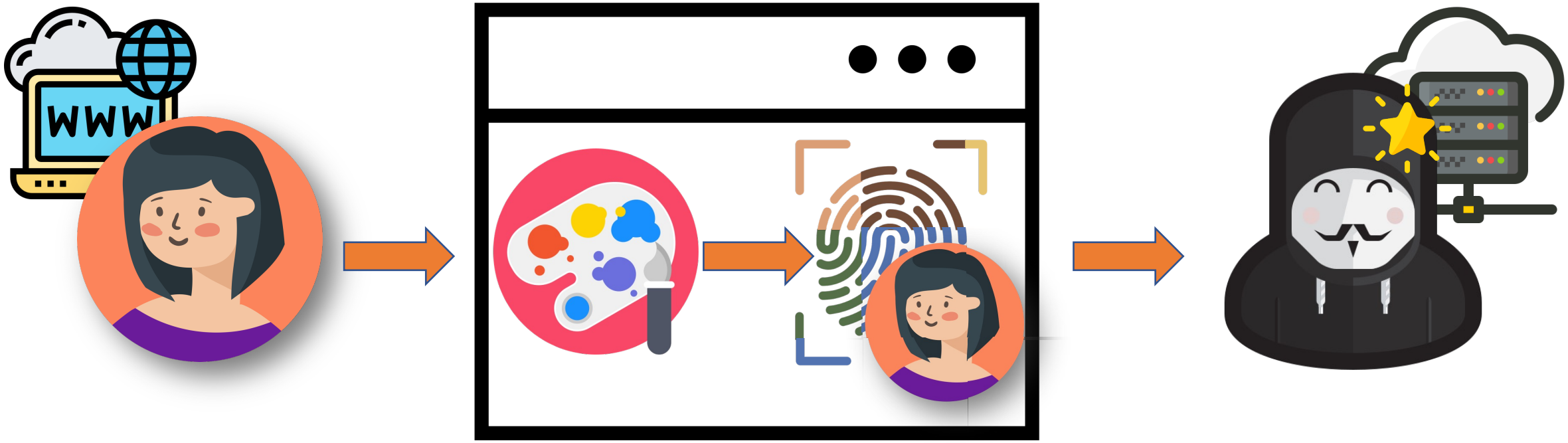
- Spoof certain APIs
- Disable JavaScript (entirely or partially)

Is fingerprinting possible without JavaScript?





Our approach



Implicit stylistic browser fingerprinting

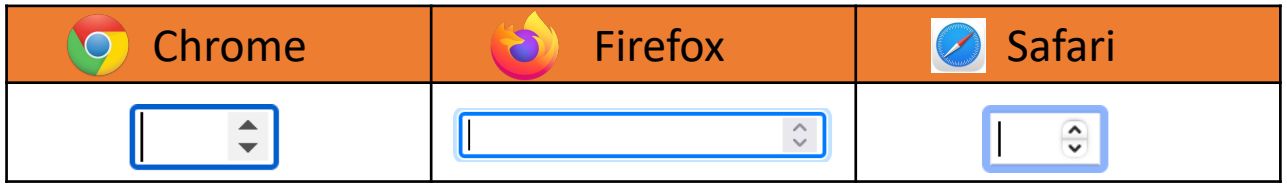
- Does not use any JavaScript
- Provides highly discriminating fingerprints

Stylistic Fingerprinting (StylisticFP)

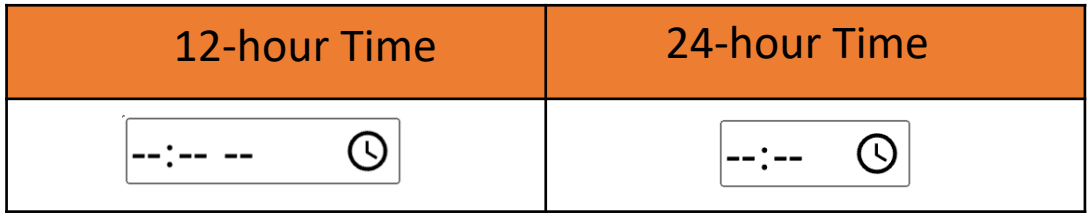
Browsers render HTML elements differently in diverse environments.

- Elements' styles depend on the underlying environment (e.g., browser, system, fonts).

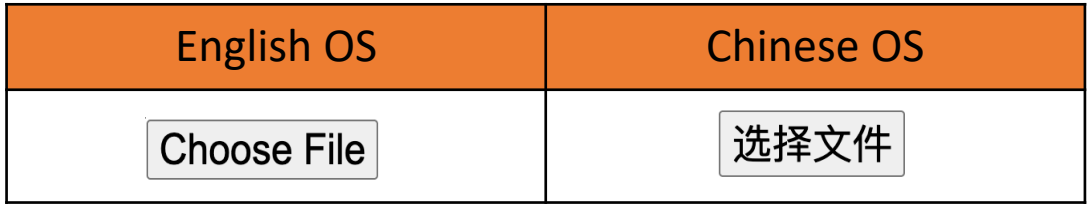
<input type="number">



<input type="time">



<input type="file">



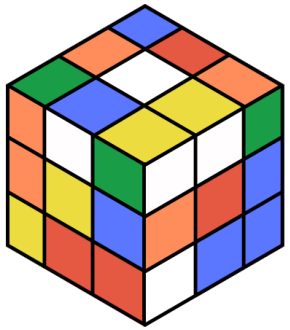
What can we use to detect the stylistic differences?

Chrome	Firefox	Safari
40px/**15**px	**183**px/**16**px	**34**px/**13**px

12-hour Time	24-hour Time
146px/32px	**99**px/32px

English OS	Chinese OS
425px/**35**px	425px/**41**px

Dimensions!



Fingerprinting attributes

Certain HTML elements have different sizes depending on certain environmental factors.

339
Fingerprinting Elements

dimensions

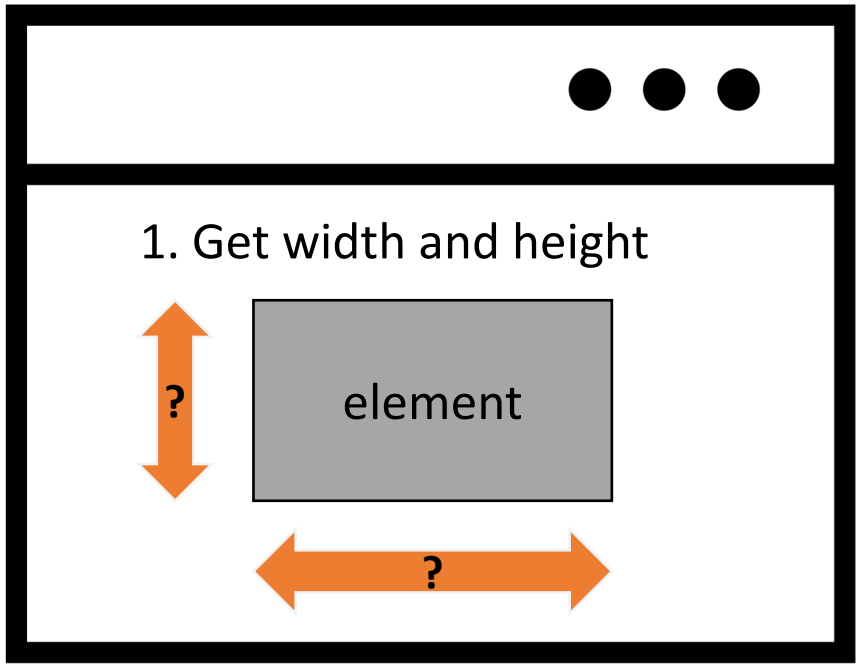
Category	Fingerprint attributes	AIU	FPJS
Environment	browser	●	●
	browser major version	●	●
	operating system	●	●
	platform	◐	◐
	operating system language		
	scrollbar settings		
	JS disabled		
Fonts	font preferences		●
	supported fonts	●	●
	supported shadow fonts		
Ad blocker	presence of ad blocker	●	
	ad blocker identification		
Media properties	screen resolution	●	●
	supported media features		◐
	media features' values		◐

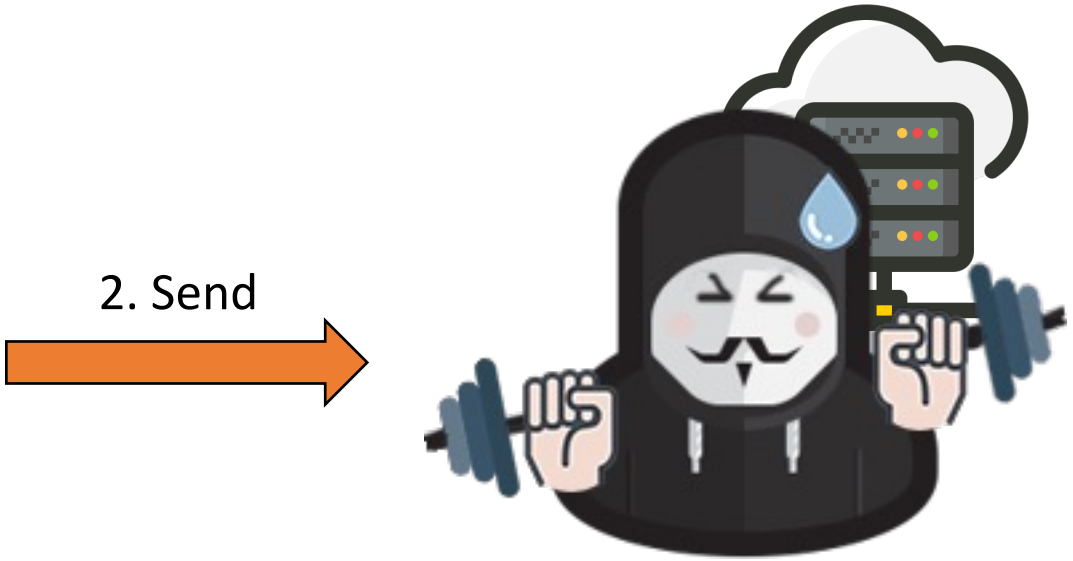
AIU: captured by AmIUnique FPJS: captured by FingerprintJS
◐ : partial feature support ●: full feature support

The Challenges

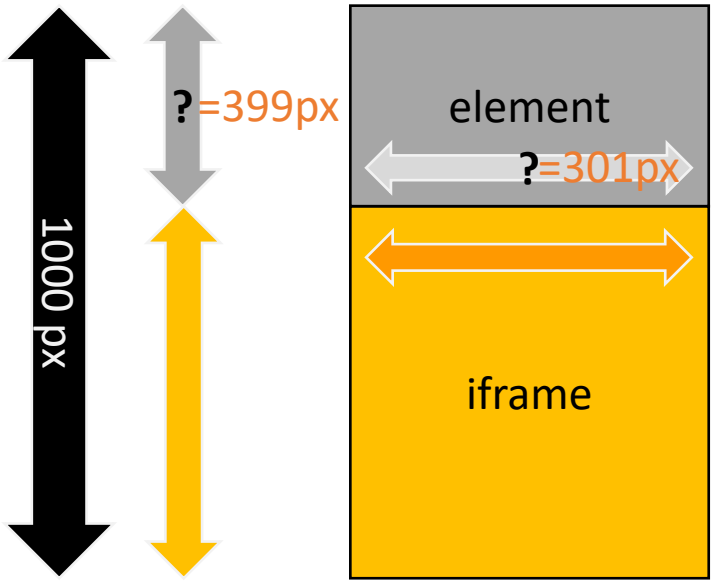
How do we obtain the rendered size of an element **without** JavaScript?

- Easy in JavaScript
- Use CSS and HTML only





Infer elements' dimensions using Media features and iframes



(a) Dimension Calculation

ElementWidth = iframeWidth
ElementHeight = 1000 – iframeHeight

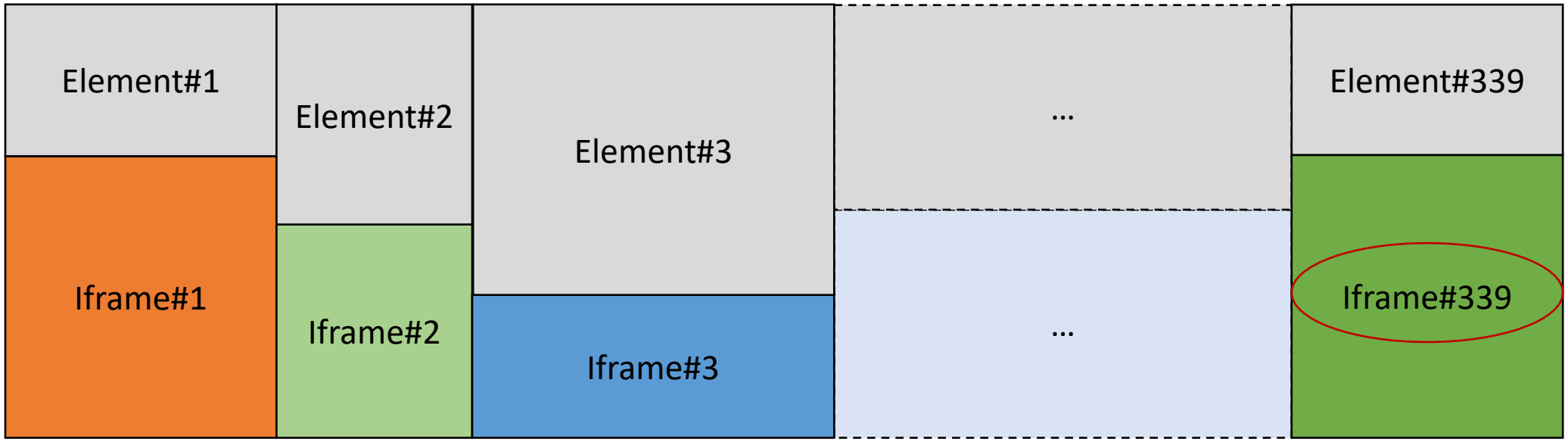
```
@media (min-width: 300px) {
   #probe { background: url(/width-300); }
}
@media (min-width: 301px) {   match
   #probe { background: url(/width-301); }
}                                   301px
...
@media (min-height: 600px) {
   #probe { background: url(/height-600); }
}
@media (min-height: 601px) {   match
   #probe { background: url(/height-601); }
}                                   601px
...
```

Dimension-based media features all refer to the dimensions of either the viewport or the device's screen—they cannot refer to a specific HTML element.

The Challenges

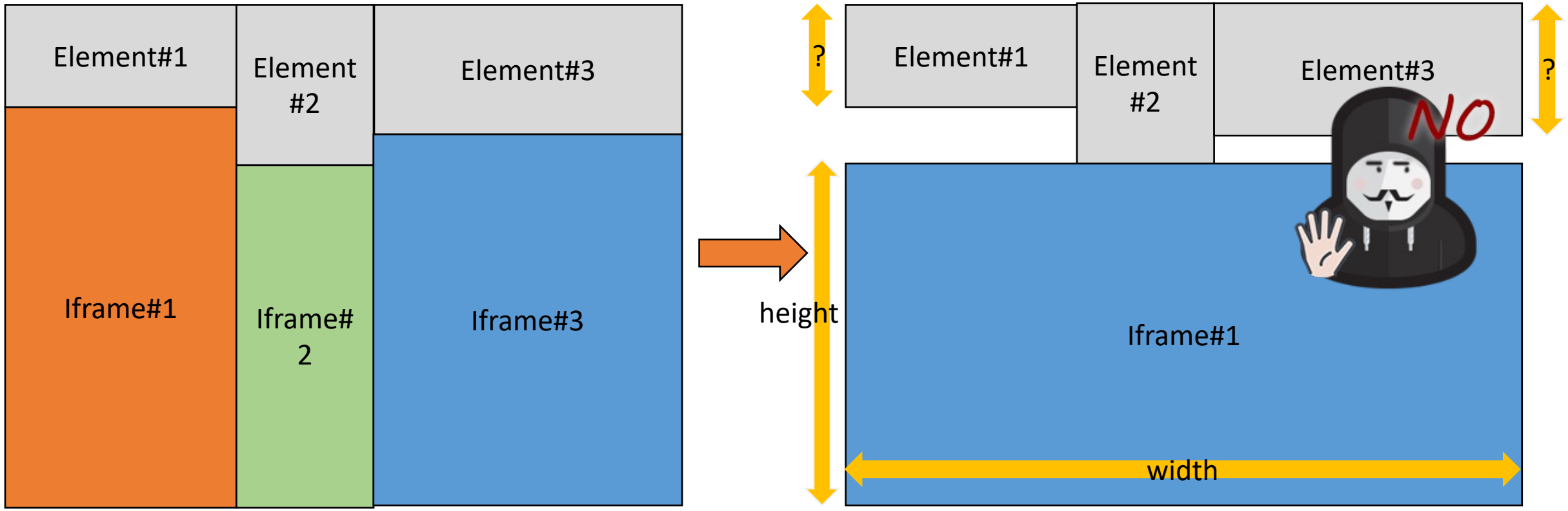
The page has 339 fingerprinting elements

- Do we need 339 iframes?
  - Use one iframe to obtain multiple elements' dimensions.



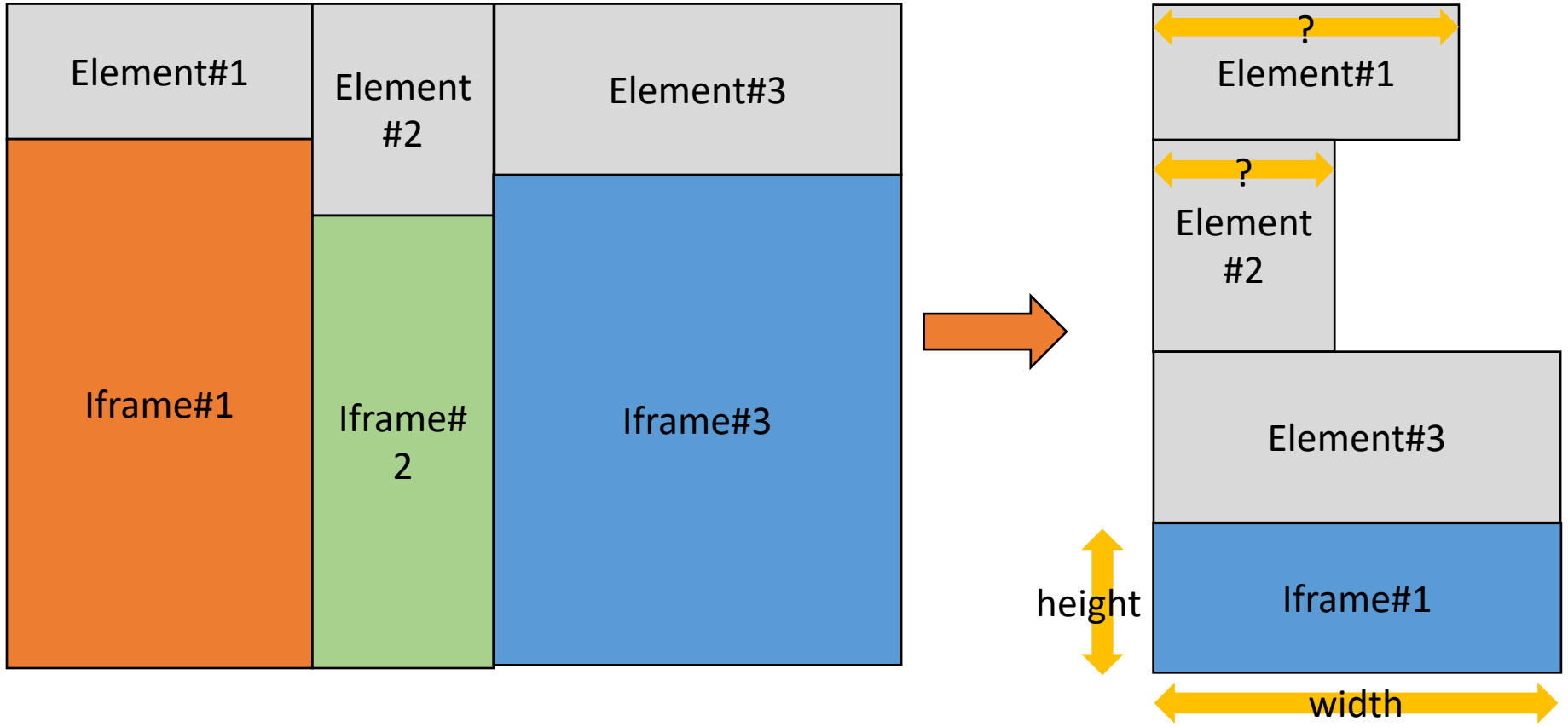
Carefully construct and arrange elements

Arranging the elements in the same row loses heights of #1 and #3.



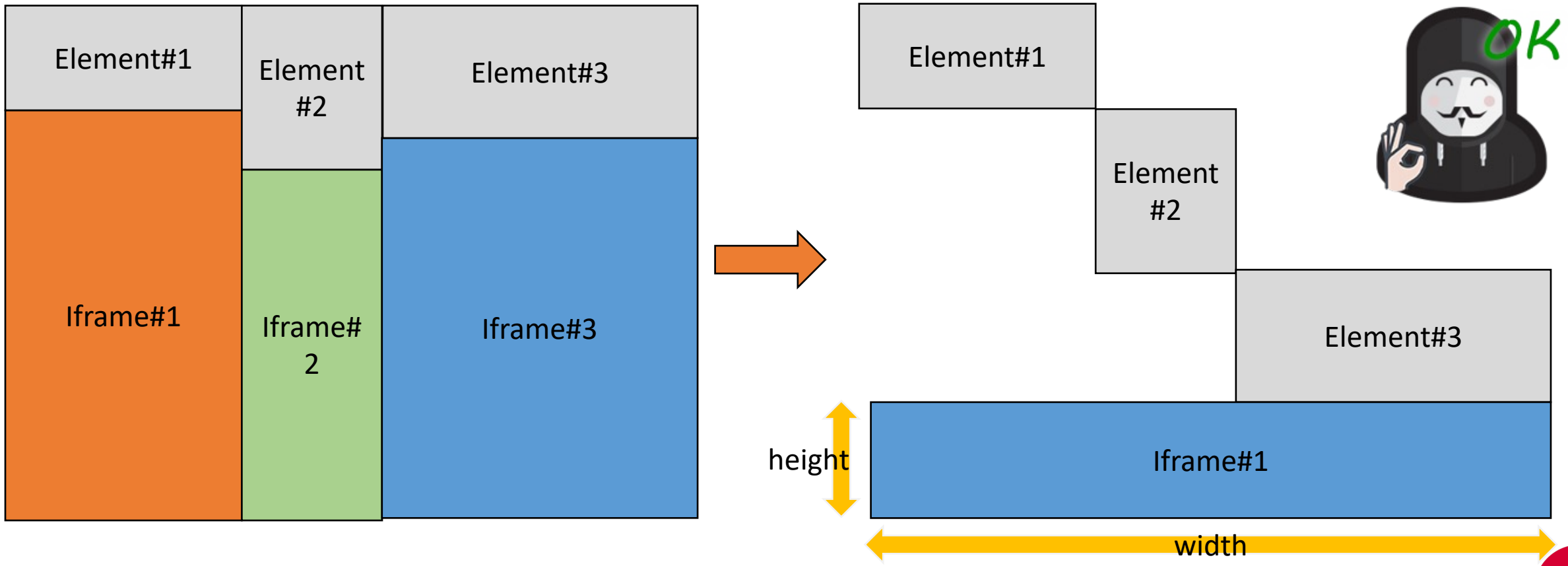
Carefully construct and arrange elements

Arranging the elements in the same column loses widths of #1 and #2.

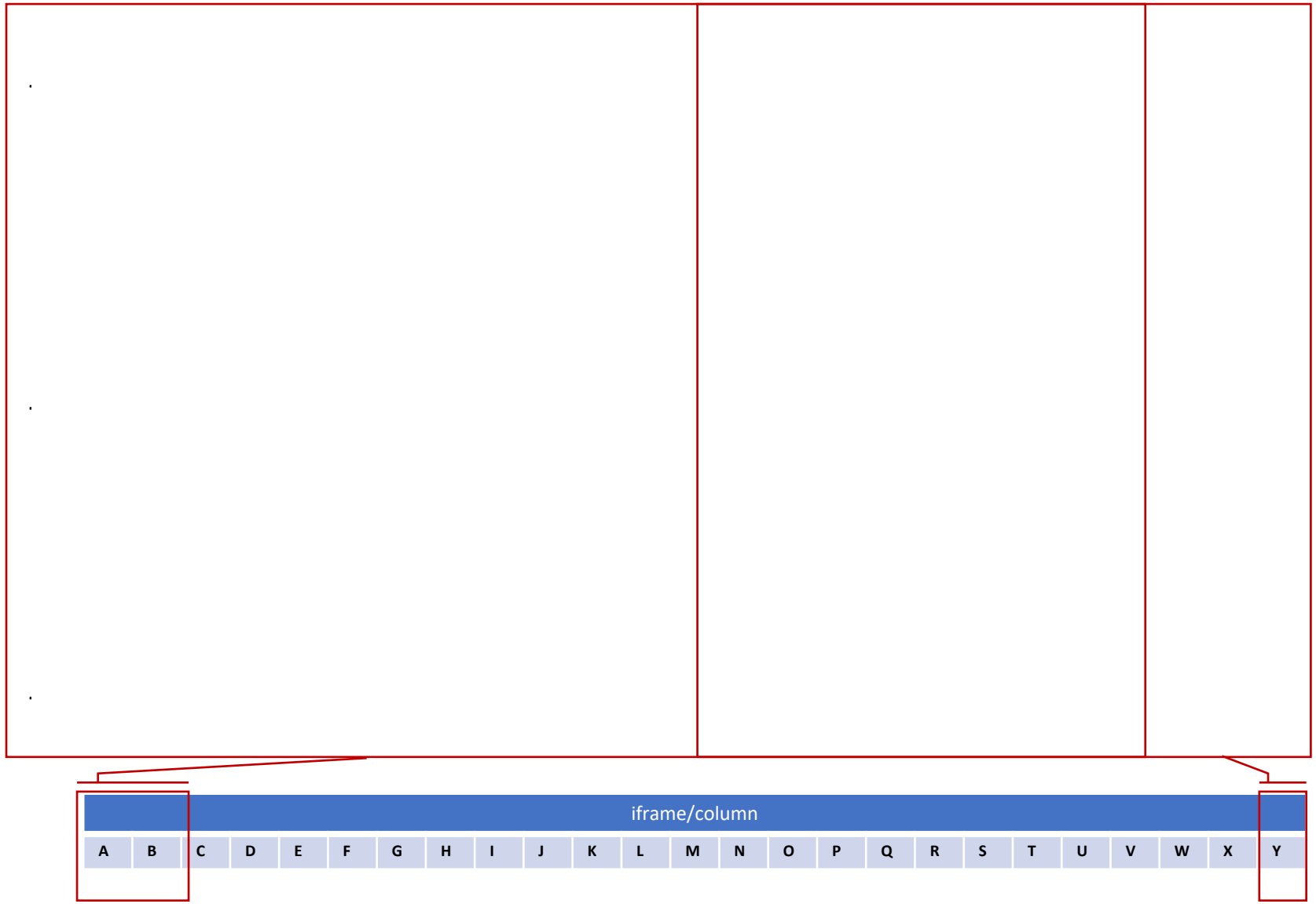


Carefully construct and arrange elements

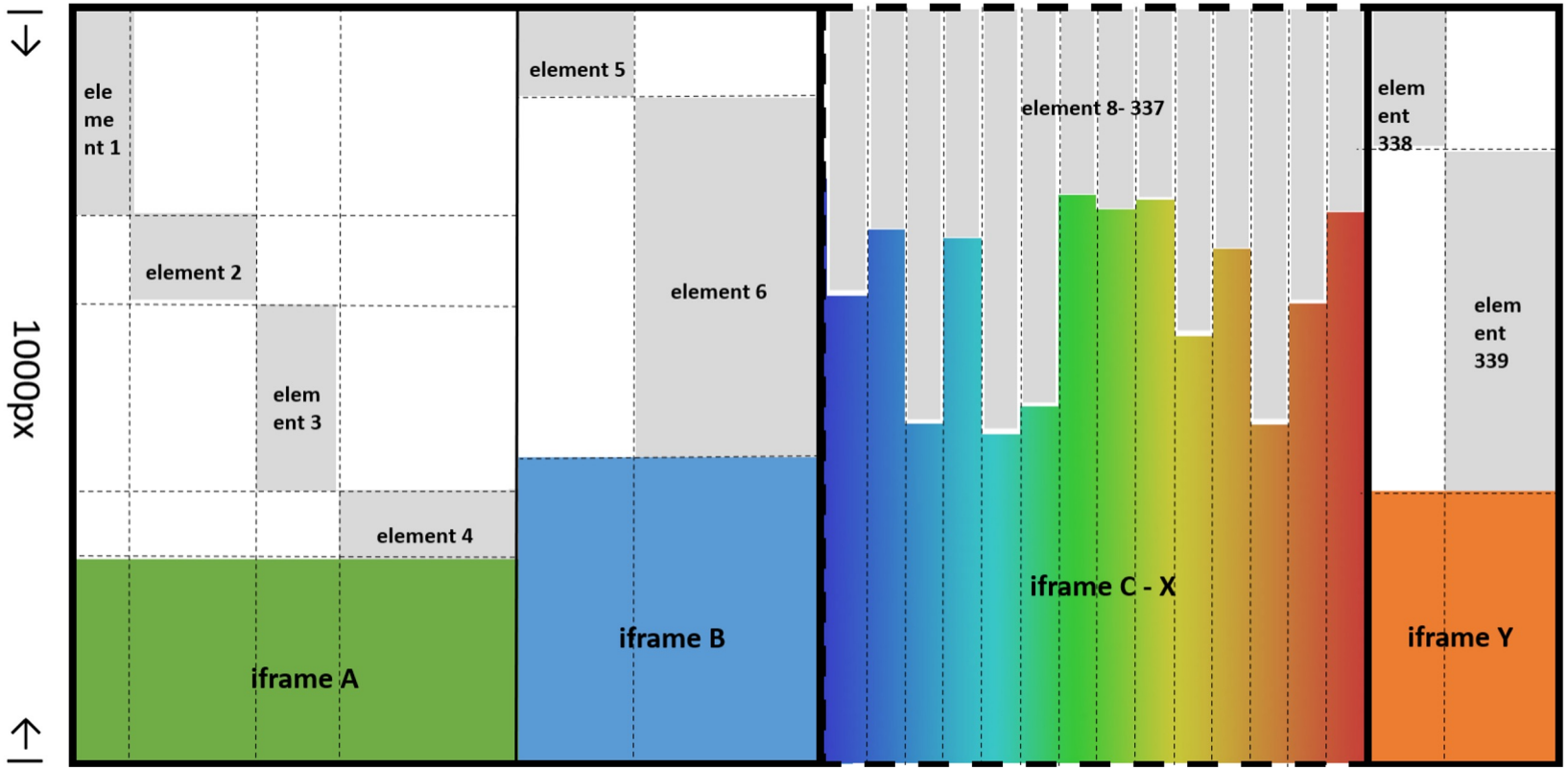
The sum of elements' widths equals the iframe's width.
The sum of elements' heights equals 1000px minus the iframe's height.

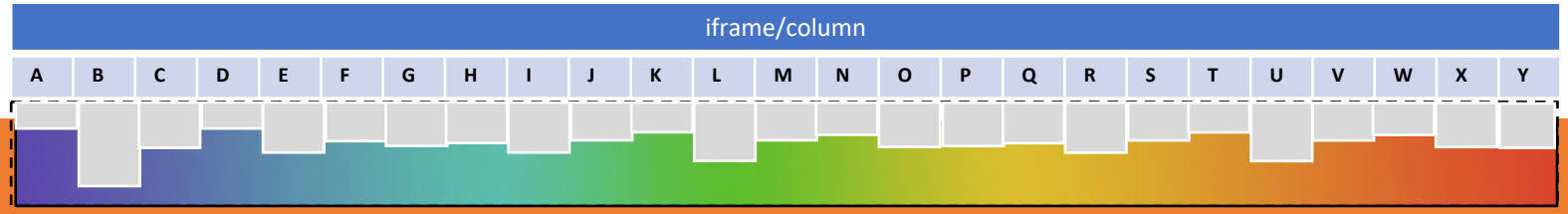


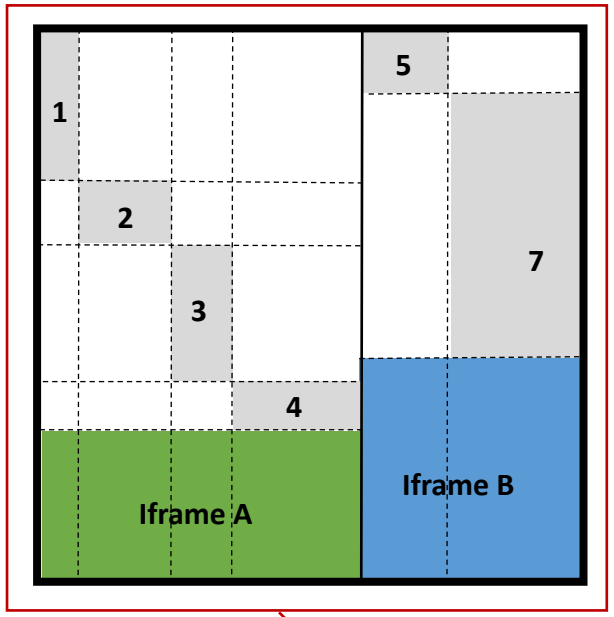
- The page only needs **25** iframes.
- All elements are placed in an 800px by 1000px iframe (main iframe) to ensure that their dimensions remain consistent across different browser window sizes.

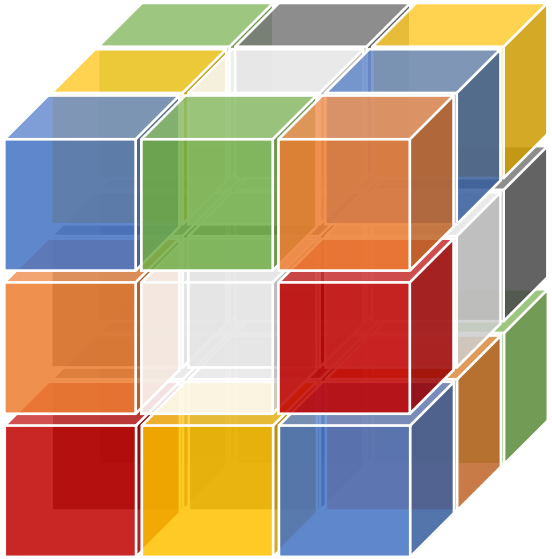


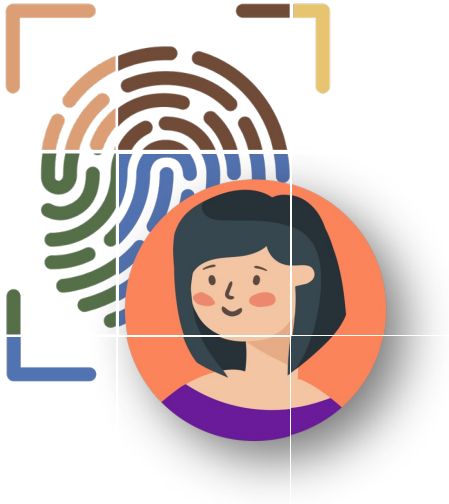
Main iframe

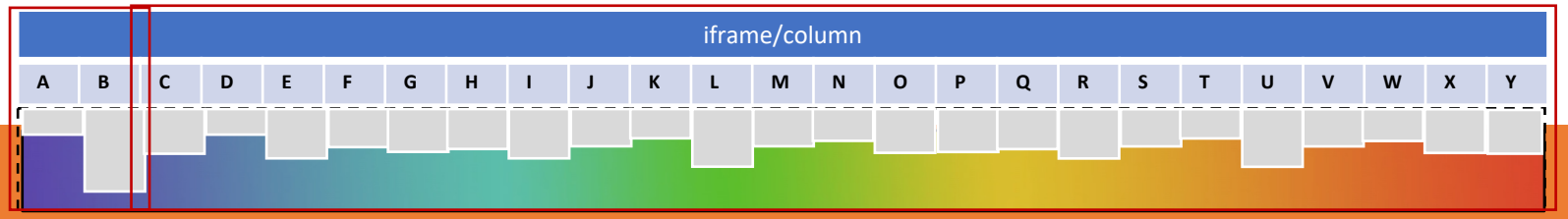

1000px
ele
me
nt 1
element 2
elem
ent 3
element 4
iframe A
element 5
element 6
iframe B
element 8- 337
iframe C - X
elem
ent
338
elem
ent
339
iframe Y


iframe/column
A B C D E F G H I J K L M N O P Q R S T U V W X Y


1
2
3
4
5
7
Iframe A
Iframe B






iframe/column
A B C D E F G H I J K L M N O P Q R S T U V W X Y

Evaluation

EFFECTIVENESS AGAINST ANTI-FINGERPRINTING BROWSERS AND TOOLS

CAPABILITY TO IDENTIFY DEVICES

Stylistic FP features effectiveness against popular countermeasures

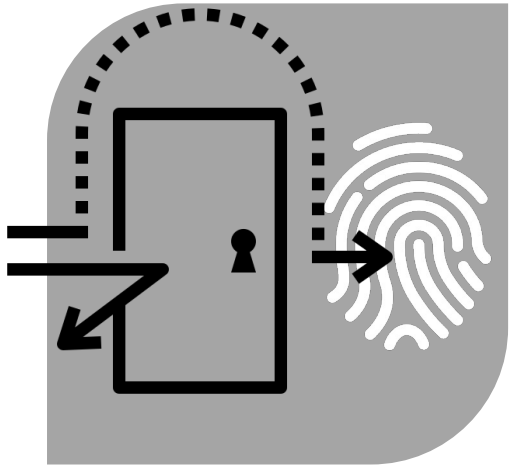
✓denotes that our technique is effective, ✗ denotes that it is ineffective, and ⊕ denotes that it is partially effective.

Feature	Brave	Tor Browser	Firefox	Firefox w/ FP Protection	Safari	Opera	Chrome w/ Anti-FP Extensions	Ghostery Browser	FP-Inspector
Browser	✓	✓	✓	✓	✓	✓	✓	✓	✓
Browser major version	✓	✓	✓	✓	✓	✓	✓	✓	✓
OS	✓	✓	✓	✓	✓	✓	✓	✓	✓
Platform	✓	✓	✓	✓	✓	✓	✓	✓	✓
OS Language									✓
Font Preferences									✓
Scrollbar Settings (OS X)									✓
Available Fonts	✓	⊕	✓	⊕	⊕	✓	✓	✓	✓
Ad blocker Use	✓	✓	✓	✓	✓	✓	✓	✓	✓
Javascript disabled	✓	✓	✓	✓	✓	✓	✓	✓	✓
Screen resolution	✓	✗	✓	✗	✓	✓	✓	✓	✓
Supported media features	✓	✓	✓	✓	✓	✓	✓	✓	✓
Media features' values	✓	⊕	✓	⊕	✓	✓	✓	✓	✓

StylisticFP is effective at bypassing the protection offered by privacy-oriented browsers, extensions, and detection tools.

We shared the source code and paper with browser venders upon requests, and received a bounty from Brave.

Evaluation



EFFECTIVENESS AGAINST ANTI-FINGERPRINTING BROWSERS AND TOOLS

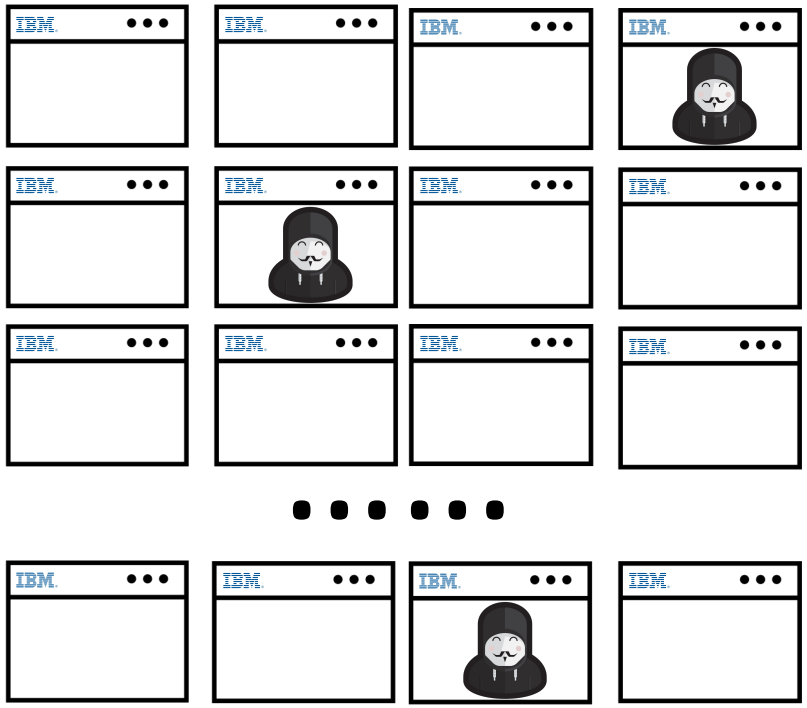
CAPABILITY TO IDENTIFY DEVICES

Pilot study

- Compared to FingerprintJS (FPJS), a prevalent state-of-the-art fingerprinting library.
- Systems deployed on three IBM intranet portals between June 1st – Aug 8th 2022”.

```
<iframe src="fp.url" style="visibility:hidden;"/>
```

- Device population is heavily skewed towards more specific, homogeneous models.



Capability to identify devices

StylisticFP

- possesses sufficient discriminative power
- outperforms FPJS in privacy-oriented browsers

TABLE 5: Comparison of uniquely identified devices by our system (**StylisticFP**) and FingerprintJS (**FPJS**) in a pilot study.

		Visits		Unique Fingerprints	
Browser	**Devices**	**Avg**	**Max**	**StylisticFP**	**FPJS**
Chromium	278	4.35	43	168	**180**
Brave	16	3.45	8	**13**	11*
Edge	41	3.83	11	**33**	32
Firefox	379	5.18	278	248	**253**
Safari	152	6.16	210	**72**	63
Total	866			534	**539**

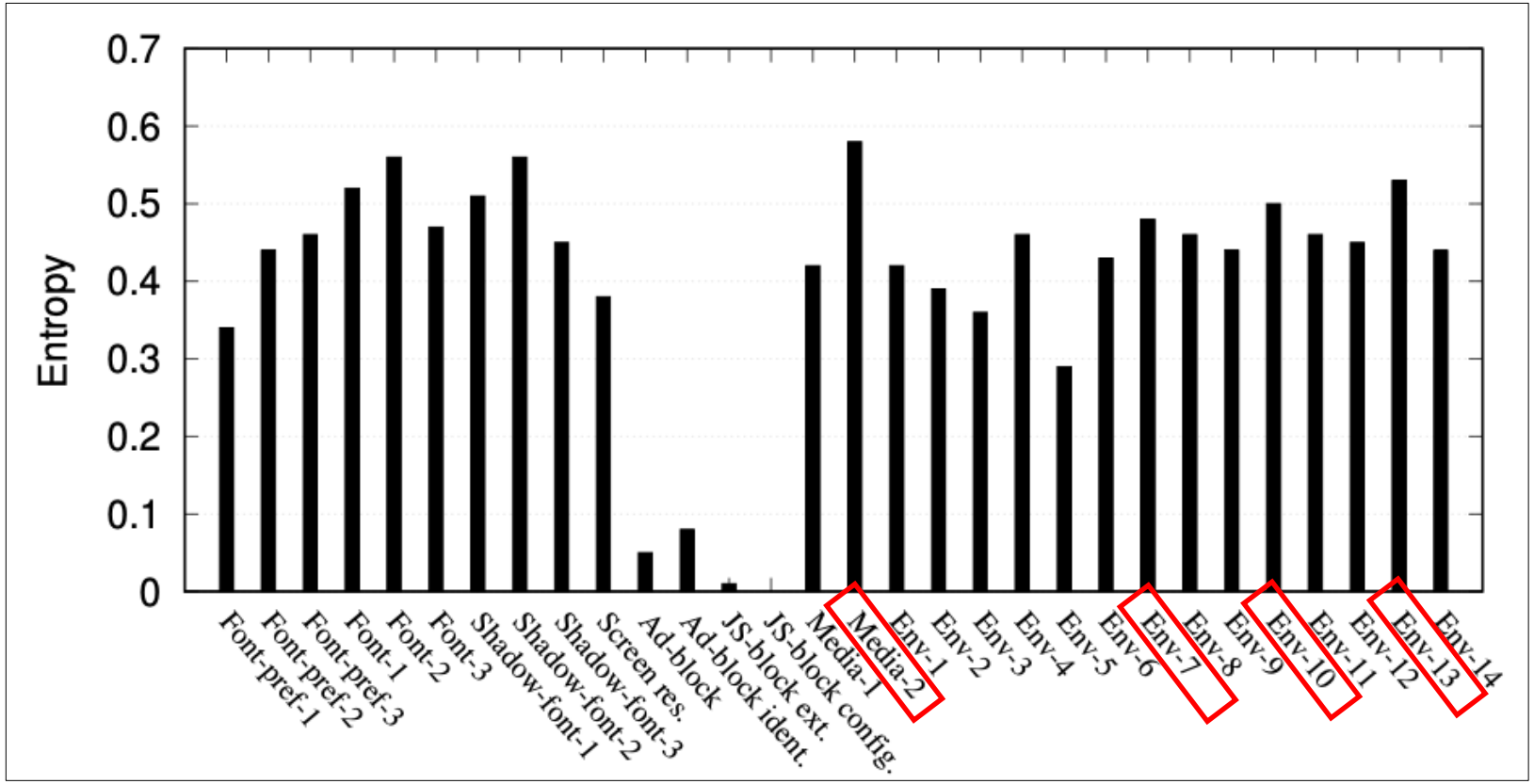
*Visits within the same session, randomized values did not change.

Entropy of stylistic fingerprinting elements

StylisticFP is comprised of high-entropy elements with more discriminating power than FPJS.

High-entropy elements:

- Media-2 probes the values of **media properties**.
- **Font** elements
- Env-7 and Env-13 probe **system language**, **region**, and **time format preferences**.
- Env-10 renders **special characters**.



The entropy is computed from **1,848** devices (including single-visit and returning devices)

Our fingerprinting system

No JavaScript needed.

Comparable discriminating power to FPJS.

Effectively bypasses state-of-the-art anti-fingerprinting defenses.

Summary

- Developed a novel fingerprinting system.
- Provided an in-depth empirical evaluation.
- Conducted a pilot study.
- Disclosed our findings to browser vendors.

Thanks!

xlin48@uic.edu