Usability of crypto API / online tracking

Mainack Mondal

CS 60081
Autumn 2022

Roadmap

- Passwords/multi factor authentications
- Usability for security developers
- Online tracking
- Privacy notices/dark patterns

Roadmap

- Passwords/multi factor authentications
- **Usability for security developers**
- Online tracking
- Privacy notices/dark patterns

Quick example of a study

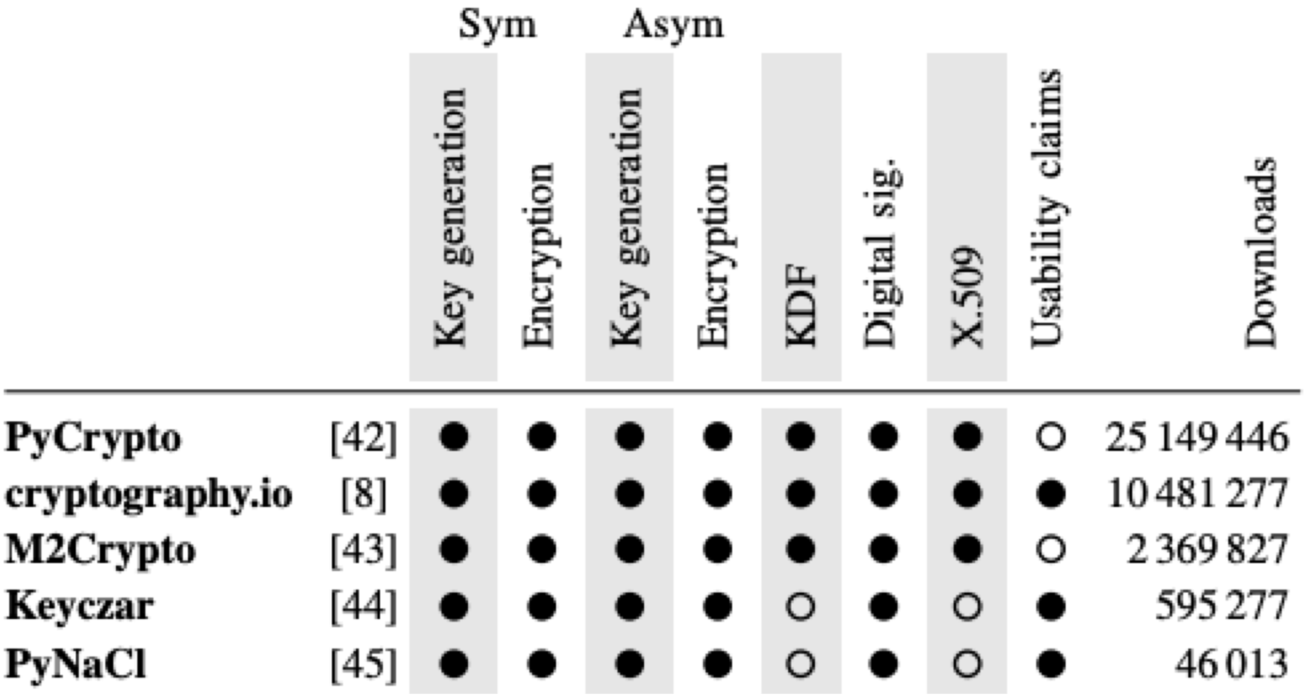
Comparing the Usability of Cryptographic APIs
https://www.cl.cam.ac.uk/~rja14/shb17/fahl.pdf

Comparing the Usability of Cryptographic APIs

- https://www.cl.cam.ac.uk/~rja14/shb17/fahl.pdf
  - First a bit about crypto
    - Encryption
    - Decryption
    - Signatures
    - Hash
  - Now, almost no-one implement these, they use libarires
    - Library calls --> cryptographic APIs

Motivation

- Wanted to check if popular python crypto libraries are actually usable



		Sym		Asym						
		Key generation	Encryption	Key generation	Encryption	KDF	Digital sig.	X.509	Usability claims	Downloads
PyCrypto	[42]	●	●	●	●	●	●	●	○	25 149 446
cryptography.io	[8]	●	●	●	●	●	●	●	●	10 481 277
M2Crypto	[43]	●	●	●	●	●	●	●	○	2 369 827
Keyczar	[44]	●	●	●	●	○	●	○	●	595 277
PyNaCl	[45]	●	●	●	●	○	●	○	●	46 013

Recruitment

- Crawled all python repositories in Github
- Extracted emails
- Email them for taking part in the survey
- Got ~200 participants
- Ecological validity – why?

Contextualization

Asked participants to imagine they were developing code for an app called CitizenMeasure,

“a new global monitoring system that will allow citizen-scientists to travel to remote locations and make measurements about such issues as water pollution, deforestation, child labor, and human trafficking. Please keep in mind that our citizen-scientists may be operating in locations that are potentially dangerous, collecting information that powerful interests want kept secret. Our citizen scientists may have their devices confiscated and hacked.”

Methodology

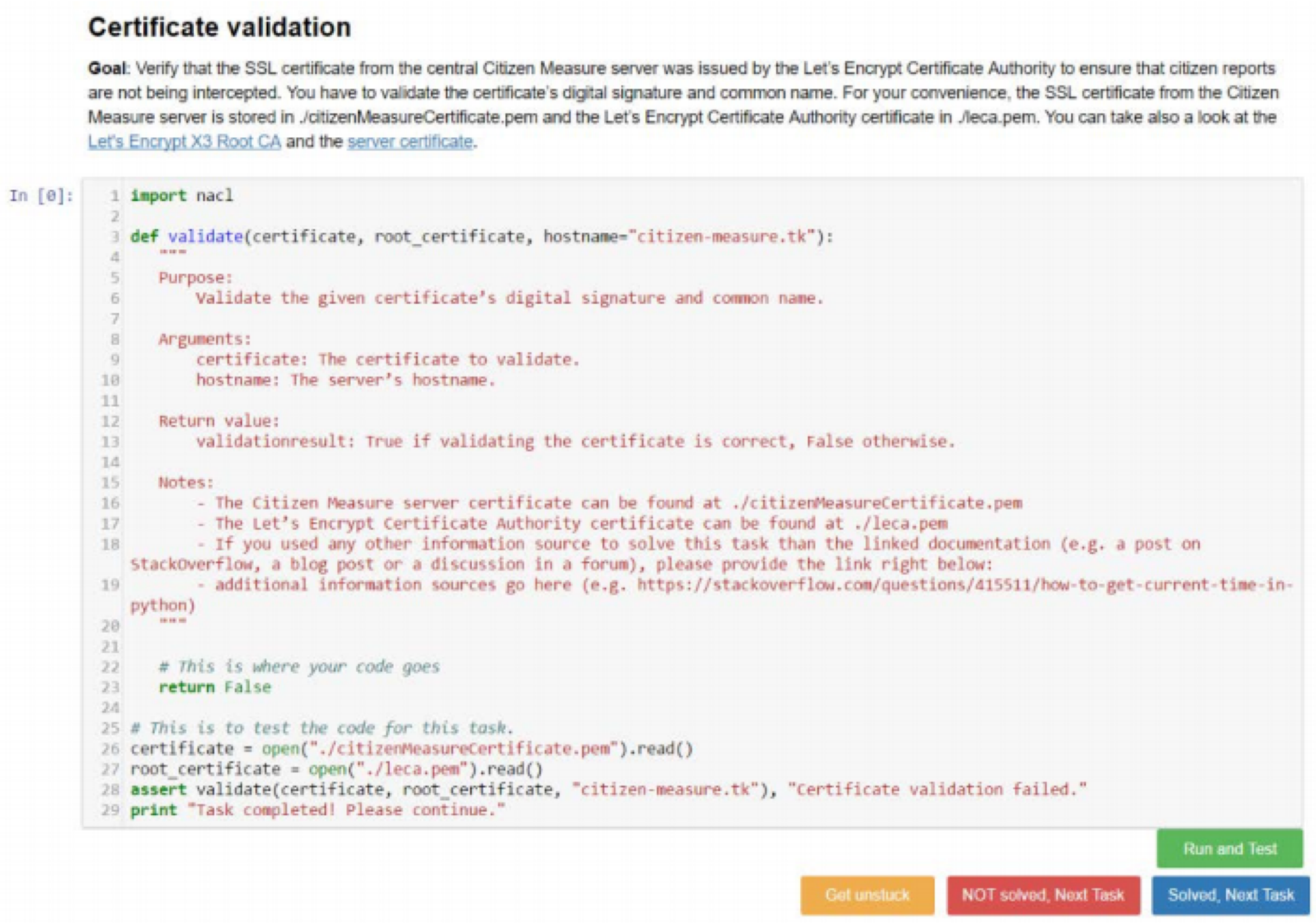
- Randomly assigned tools to the developers
  - Between-subjects study
- Ask them to perform tasks online (py notebook)
  - Online study
  - Contextualization
- Qualitative analysis
  - Took the developer’s solutions
  - Then two authors labeled them as functional, secure
  - Then they used statistics to measure usability!

Tasks

- Two symmetric encryption tasks
  - generating an encryption key and storing it securely in a password-protected file
  - using the key to encrypt and decrypt text

- Three asymmetric encryption tasks
  - generating a key pair and storing the private key securely
  - using the public key to encrypt and the private key to decrypt
  - validating an X.509 certificate.

Task example



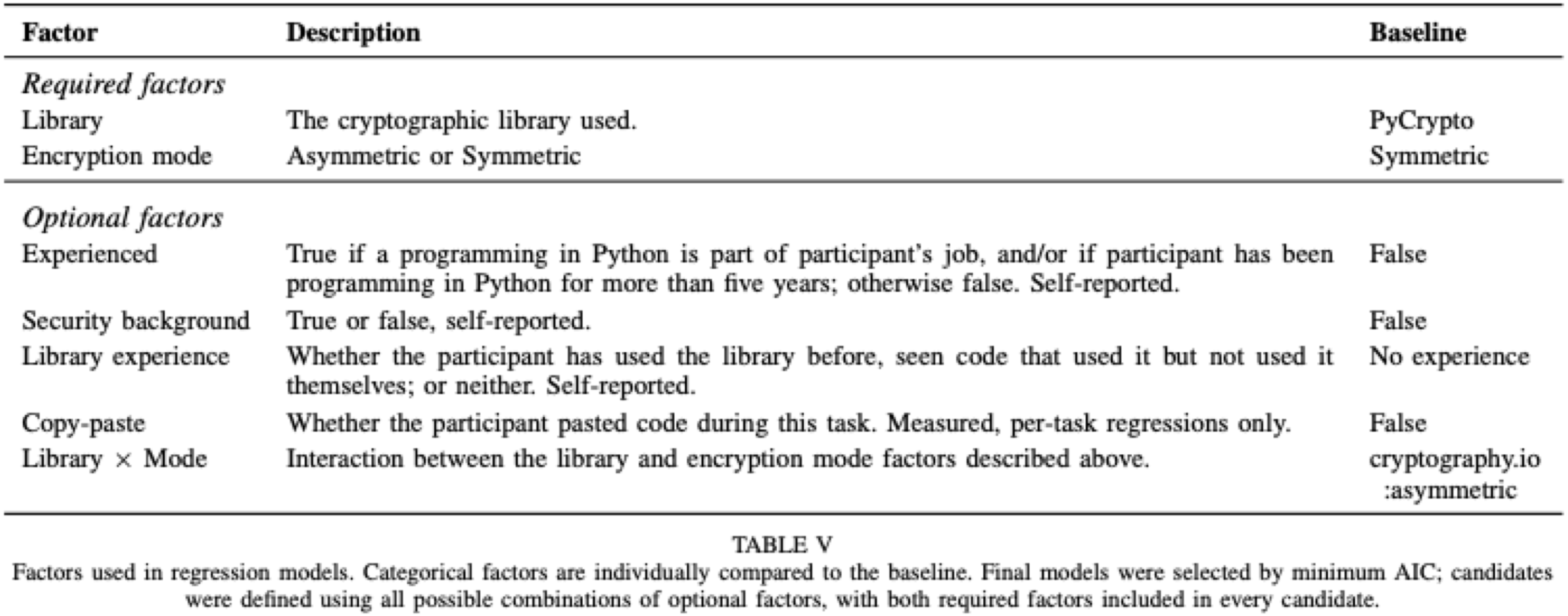
Certificate validation

Goal: Verify that the SSL certificate from the central Citizen Measure server was issued by the Let's Encrypt Certificate Authority to ensure that citizen reports are not being intercepted. You have to validate the certificate's digital signature and common name. For your convenience, the SSL certificate from the Citizen Measure server is stored in ./citizenMeasureCertificate.pem and the Let's Encrypt Certificate Authority certificate in ./leca.pem. You can take also a look at the Let's Encrypt X3 Root CA and the server certificate.

```
import nacl

def validate(certificate, root_certificate, hostname="citizen-measure.tk"):
    """
    Purpose:
        Validate the given certificate's digital signature and common name.

    Arguments:
        certificate: The certificate to validate.
        hostname: The server's hostname.

    Return value:
        validationresult: True if validating the certificate is correct, False otherwise.

    Notes:
        - The Citizen Measure server certificate can be found at ./citizenMeasureCertificate.pem
        - The Let's Encrypt Certificate Authority certificate can be found at ./leca.pem
        - If you used any other information source to solve this task than the linked documentation (e.g. a post on StackOverflow, a blog post or a discussion in a forum), please provide the link right below:
        - additional information sources go here (e.g. https://stackoverflow.com/questions/415511/how-to-get-current-time-in-python)
    """

    # This is where your code goes
    return False

# This is to test the code for this task.
certificate = open("./citizenMeasureCertificate.pem").read()
root_certificate = open("./leca.pem").read()
assert validate(certificate, root_certificate, "citizen-measure.tk"), "Certificate validation failed."
print "Task completed! Please continue."
```

Fig. 1. An example of the study's task interface.

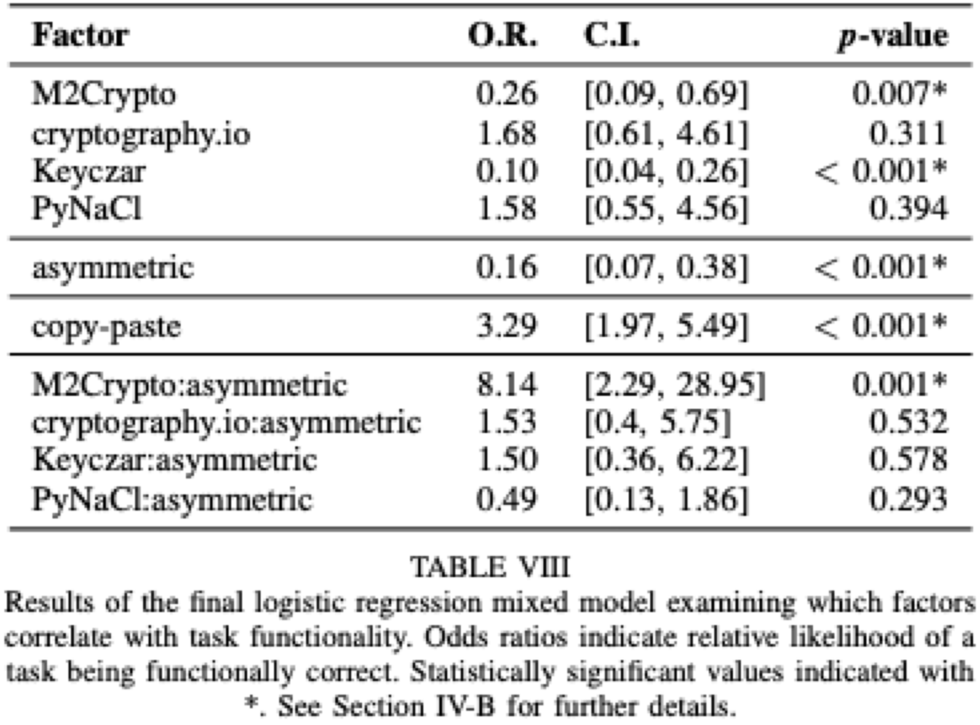
Analysis: Regression



Factor	Description	Baseline
Required factors		
Library	The cryptographic library used.	PyCrypto
Encryption mode	Asymmetric or Symmetric	Symmetric
Optional factors		
Experienced	True if a programming in Python is part of participant's job, and/or if participant has been programming in Python for more than five years; otherwise false. Self-reported.	False
Security background	True or false, self-reported.	False
Library experience	Whether the participant has used the library before, seen code that used it but not used it themselves; or neither. Self-reported.	No experience
Copy-paste	Whether the participant pasted code during this task. Measured, per-task regressions only.	False
Library × Mode	Interaction between the library and encryption mode factors described above.	cryptography.io :asymmetric

TABLE V
Factors used in regression models. Categorical factors are individually compared to the baseline. Final models were selected by minimum AIC; candidates were defined using all possible combinations of optional factors, with both required factors included in every candidate.

Result



Factor	O.R.	C.I.	*p*-value
M2Crypto	0.26	[0.09, 0.69]	0.007*
cryptography.io	1.68	[0.61, 4.61]	0.311
Keyczar	0.10	[0.04, 0.26]	< 0.001*
PyNaCl	1.58	[0.55, 4.56]	0.394
asymmetric	0.16	[0.07, 0.38]	< 0.001*
copy-paste	3.29	[1.97, 5.49]	< 0.001*
M2Crypto:asymmetric	8.14	[2.29, 28.95]	0.001*
cryptography.io:asymmetric	1.53	[0.4, 5.75]	0.532
Keyczar:asymmetric	1.50	[0.36, 6.22]	0.578
PyNaCl:asymmetric	0.49	[0.13, 1.86]	0.293

TABLE VIII

Results of the final logistic regression mixed model examining which factors correlate with task functionality. Odds ratios indicate relative likelihood of a task being functionally correct. Statistically significant values indicated with *. See Section IV-B for further details.

Roadmap

- Passwords/multi factor authentications
- Usability for security developers
- Online tracking
- Privacy notices/dark patterns

Behavioral targeting/tracking

Behavioral targeting/tracking

Scenario: You are visiting a website

- First party: the website your are visiting
- Second party: You
- Third party: Other sites the first site as a result of your visit to the site. Why will it happen?

Online tracking

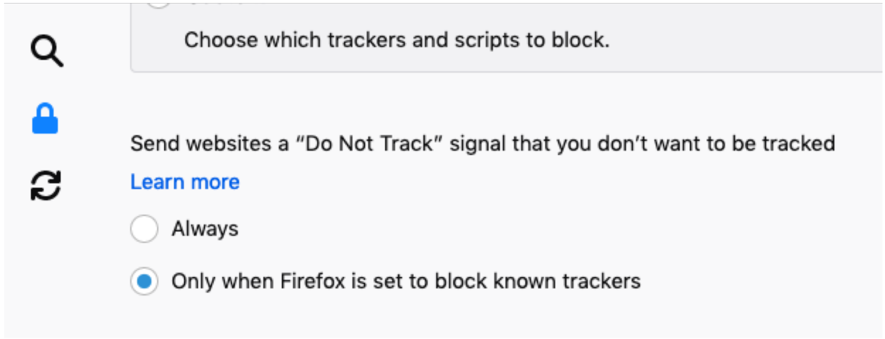
- First party tracking
  - E.g., Google track your search results
- Solution: Use duckduckgo

- Stopping Third party tracking
  - Much harder…
  - But why would a third party track a user?

Do not track

- Proposed standard
- User checks a box
- Browser sends "do not track" to website
- Website stops "tracking"
  - What does that even mean?
  - cookies, javascript?

- Discontinued in apple, why?



Choose which trackers and scripts to block.

Send websites a "Do Not Track" signal that you don't want to be tracked

Learn more

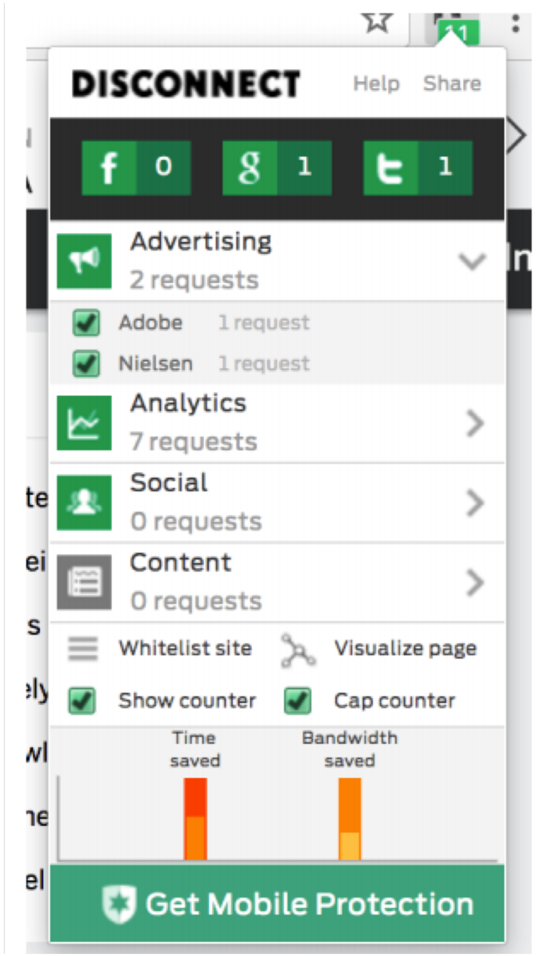
○ Always

● Only when Firefox is set to block known trackers

Tools to stop tracking

- Browser privacy settings
    - Blocking cookies
    - P3P
- Browser extensions
- Opt-out cookies
- Digital Advertising Alliance (DAA) adchoices and associated opt-out pages

Extensions: Disconnect



DISCONNECT Help Share

f 0 g 1 t 1

Advertising
2 requests

☑ Adobe 1 request

☑ Nielsen 1 request

Analytics
7 requests

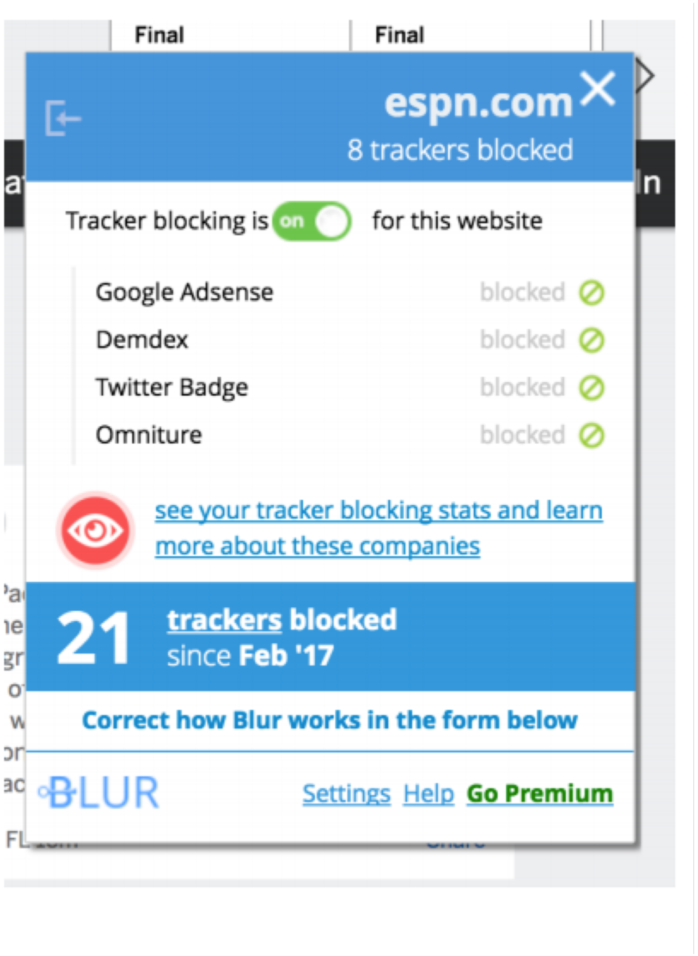
Social
0 requests

Content
0 requests

Whitelist site Visualize page

☑ Show counter ☑ Cap counter

Get Mobile Protection



espn.com
8 trackers blocked

Tracker blocking is on for this website

Google Adsense	blocked
Demdex	blocked
Twitter Badge	blocked
Omniture	blocked

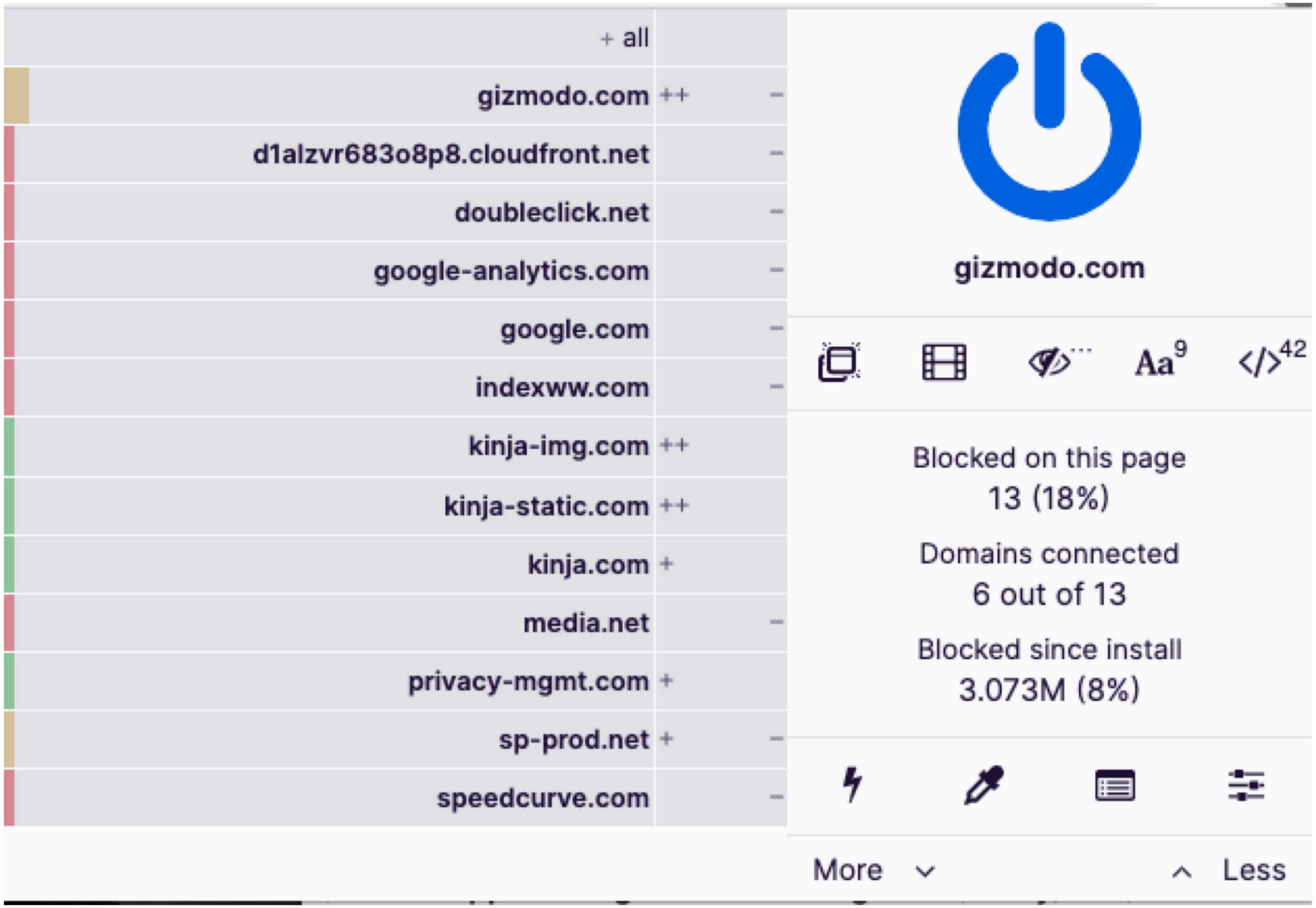
see your tracker blocking stats and learn more about these companies

21 trackers blocked since Feb '17

Correct how Blur works in the form below

BLUR Settings Help Go Premium

Extensions: Ublock origin



+ all		
gizmodo.com	++	−
d1alzvr683o8p8.cloudfront.net		−
doubleclick.net		−
google-analytics.com		−
google.com		−
indexww.com		−
kinja-img.com	++	
kinja-static.com	++	
kinja.com	+	
media.net		−
privacy-mgmt.com	+	
sp-prod.net	+	−
speedcurve.com		−

gizmodo.com

Blocked on this page
13 (18%)

Domains connected
6 out of 13

Blocked since install
3.073M (8%)

Browser fingerprinting

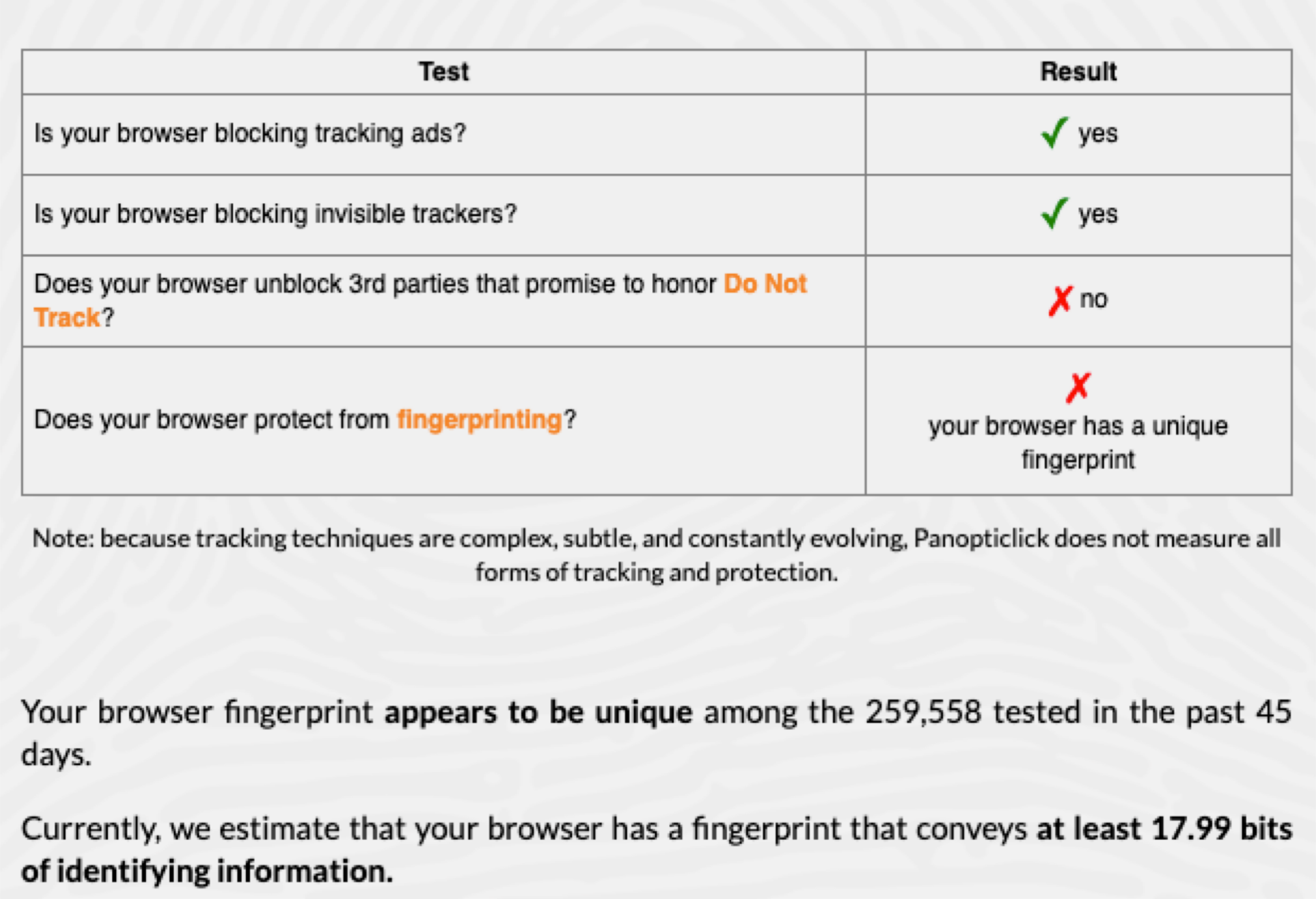
- Use features of your browser that are relatively unique to your machine
    - Fonts
    - GPU model anti aliasing (canvas fingerprinting)
    - User agent string
    - IP is often not used (why?)

Browser fingerprinting

- Use features of your browser that are relatively unique to your machine
  - Fonts
  - GPU model anti aliasing (canvas fingerprinting)
  - User agent string
  - IP is often not used (why?)

Check: https://panopticlick.eff.org/

Browser fingerprinting



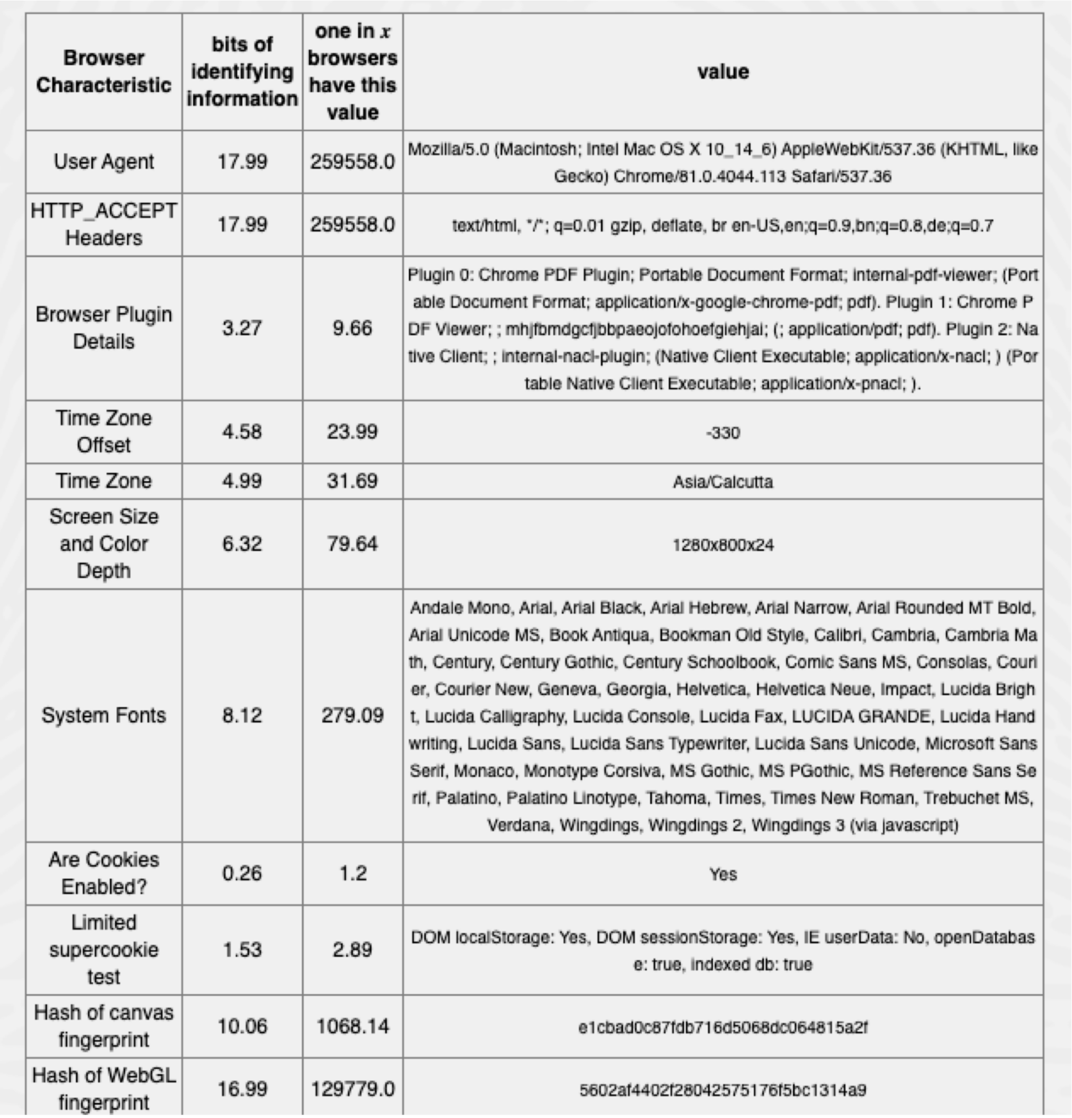
Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 259,558 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.99 bits of identifying information.**

Browser fingerprinting



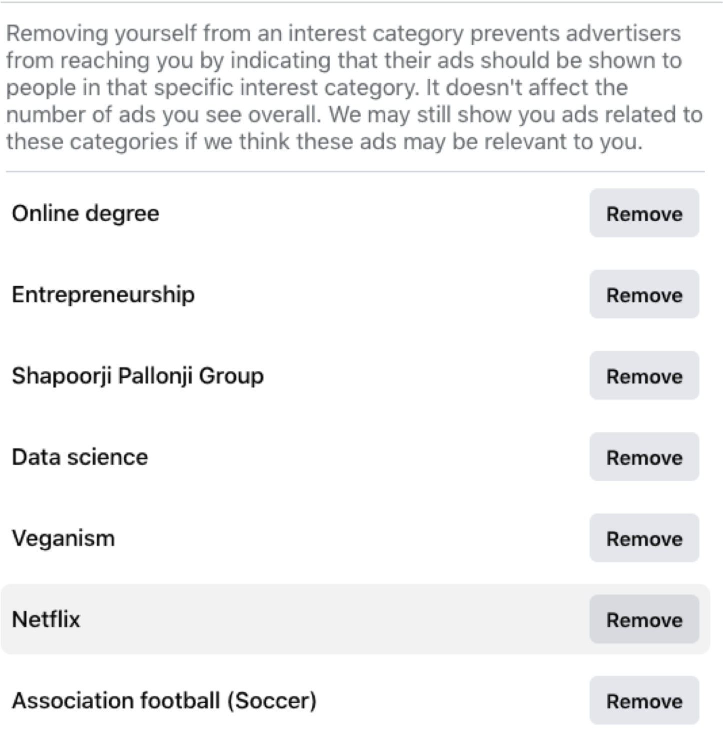
Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	17.99	259558.0	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.113 Safari/537.36
HTTP_ACCEPT Headers	17.99	259558.0	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.9,bn;q=0.8,de;q=0.7
Browser Plugin Details	3.27	9.66	Plugin 0: Chrome PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf). Plugin 2: Native Client; ; internal-nacl-plugin; (Native Client Executable; application/x-nacl;) (Portable Native Client Executable; application/x-pnacl;).
Time Zone Offset	4.58	23.99	-330
Time Zone	4.99	31.69	Asia/Calcutta
Screen Size and Color Depth	6.32	79.64	1280x800x24
System Fonts	8.12	279.09	Andale Mono, Arial, Arial Black, Arial Hebrew, Arial Narrow, Arial Rounded MT Bold, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Geneva, Georgia, Helvetica, Helvetica Neue, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, LUCIDA GRANDE, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monaco, Monotype Corsiva, MS Gothic, MS PGothic, MS Reference Sans Serif, Palatino, Palatino Linotype, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Are Cookies Enabled?	0.26	1.2	Yes
Limited supercookie test	1.53	2.89	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: true, indexed db: true
Hash of canvas fingerprint	10.06	1068.14	e1cbad0c87fdb716d5068dc064815a2f
Hash of WebGL fingerprint	16.99	129779.0	5602af4402f28042575176f5bc1314a9

Tracking in social media

- Go to https://www.facebook.com/adpreferences/ad_settings
- Then “Categories used to reach you” → “Interest categories”

Tracking in social media

- Go to https://www.facebook.com/adpreferences/ad_settings
- Then “Categories used to reach you” → “Interest categories”



Removing yourself from an interest category prevents advertisers from reaching you by indicating that their ads should be shown to people in that specific interest category. It doesn't affect the number of ads you see overall. We may still show you ads related to these categories if we think these ads may be relevant to you.

Online degree

Entrepreneurship

Shapoorji Pallonji Group

Data science

Veganism

Netflix

Association football (Soccer)

How to help users?

- Bringing transparency to the web