Phish in Sheep’s Clothing

Risk-Based Authentication

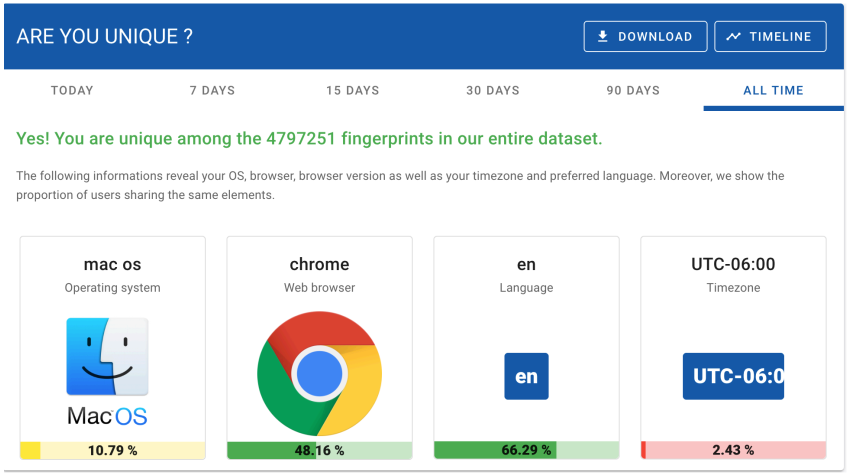
- A site can compute *risk* factor for authenticating a user
  - Based on behavior, action impact, location, *browser features*
- Use different authentication styles depending on risk
  - No auth
  - Password
  - 2FA
  - Re-authenticate (password, 2FA)
- Why?

Study Browser Fingerprinting in RBA

- Q1: How do websites use browser FP in RBA?
  - Bypassing 2FA
- Q2: How easy is it to for an attacker to fool browser FP?
  - Mimic browser fingeprint

Browser Fingerprinting

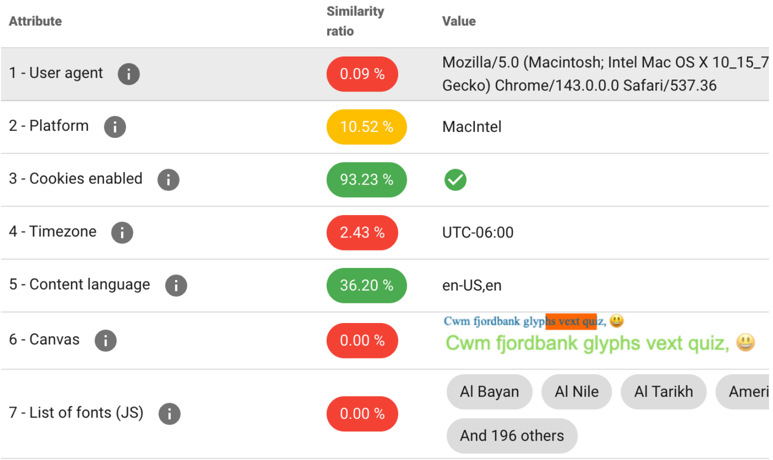
- Use Javascript APIs to identify features of browser that:
  - Vary across users / devices
  - Remain stable for a single user
- Heavily used in both anti-fraud and ad tracking



Yes! You are unique among the 4797251 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

mac os	chrome	en	UTC-06:00
Operating system	Web browser	Language	Timezone
10.79 %	48.16 %	66.29 %	2.43 %



Attribute	Similarity ratio	Value
1 - User agent	0.09 %	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7 Gecko) Chrome/143.0.0.0 Safari/537.36
2 - Platform	10.52 %	MacIntel
3 - Cookies enabled	93.23 %	✓
4 - Timezone	2.43 %	UTC-06:00
5 - Content language	36.20 %	en-US,en
6 - Canvas	0.00 %	Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃
7 - List of fonts (JS)	0.00 %	Al Bayan Al Nile Al Tarikh Ameri And 196 others

Spoofing Workflow

- FP-Extractor: identify fingerprinting code from a target website
  - Based on previous research on fingerprinting detection
- Fingerprint capture
  - Deploy on phishing site
  - Capture values returned by APIs
- FP-Spoofer
  - Interpose on JS APIs to return spoofed values

Experimental Design

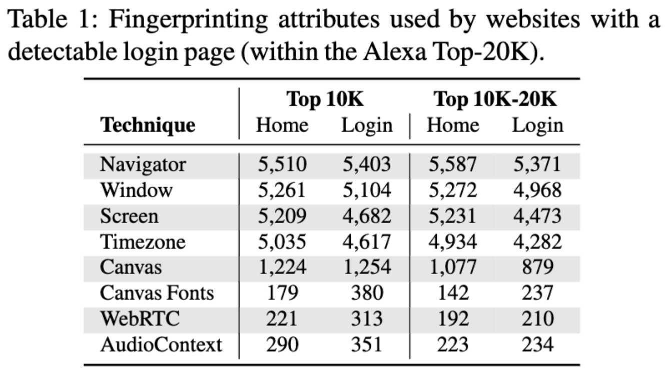


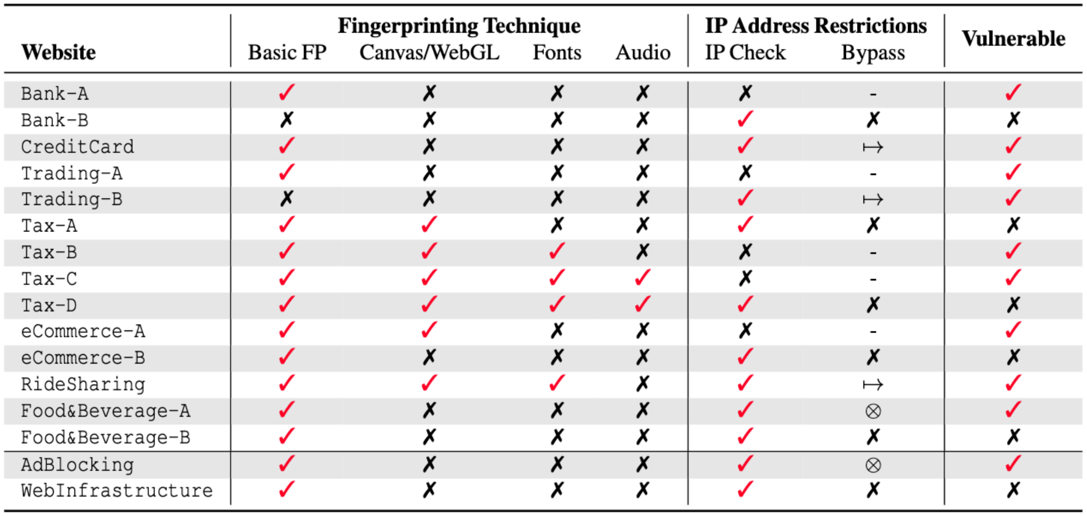
Table 1: Fingerprinting attributes used by websites with a detectable login page (within the Alexa Top-20K).

Technique	**Top 10K** Home	Login	**Top 10K-20K** Home	Login
Navigator	5,510	5,403	5,587	5,371
Window	5,261	5,104	5,272	4,968
Screen	5,209	4,682	5,231	4,473
Timezone	5,035	4,617	4,934	4,282
Canvas	1,224	1,254	1,077	879
Canvas Fonts	179	380	142	237
WebRTC	221	313	192	210
AudioContext	290	351	223	234

- Scan Alexa top-20K
  - Find login pages
  - Note usage of fingerprinting APIs
  - Heuristic search for 2FA usage
- Select 300 sites to examine
  - 16 use browser FP to recognize users, skip 2FA
  - Cookies are used by others

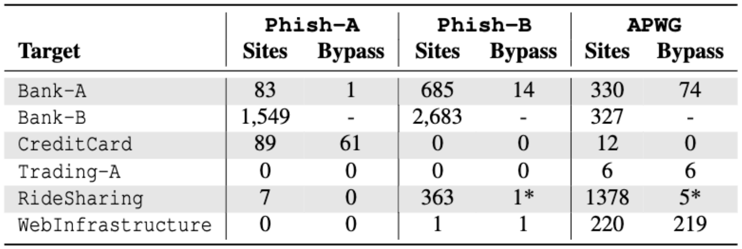
Results

- Fingerprints often augmented with IP check
  - In some cases can be bypassed
- Fingerprints also used for email notification alerts
- Some evidence of phishing sites collecting fingerprints!



Website	Fingerprinting Technique				IP Address Restrictions		Vulnerable
	Basic FP	Canvas/WebGL	Fonts	Audio	IP Check	Bypass	
Bank-A	✓	✗	✗	✗	✗	-	✓
Bank-B	✗	✗	✗	✗	✓	✗	✗
CreditCard	✓	✗	✗	✗	✓	↦	✓
Trading-A	✓	✗	✗	✗	✗	-	✓
Trading-B	✗	✗	✗	✗	✓	↦	✓
Tax-A	✓	✓	✗	✗	✓	✗	✗
Tax-B	✓	✓	✓	✗	✗	-	✓
Tax-C	✓	✓	✓	✓	✗	-	✓
Tax-D	✓	✓	✓	✓	✓	✗	✗
eCommerce-A	✓	✓	✗	✗	✗	-	✓
eCommerce-B	✓	✗	✗	✗	✓	✗	✗
RideSharing	✓	✓	✓	✗	✓	↦	✓
Food&Beverage-A	✓	✗	✗	✗	✓	⊗	✓
Food&Beverage-B	✓	✗	✗	✗	✓	✗	✗
AdBlocking	✓	✗	✗	✗	✓	⊗	✓
WebInfrastructure	✓	✗	✗	✗	✓	✗	✗

Table 5: Phishing sites that obtain all the necessary browser fingerprints for bypassing 2FA in the target sites. "*" indicates a mismatch in fingerprinting function arguments.

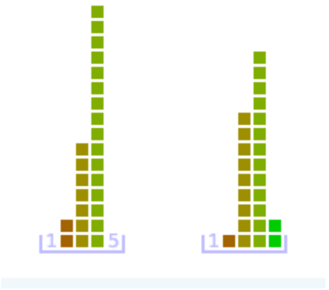


Target	Phish-A		Phish-B		APWG	
	Sites	Bypass	Sites	Bypass	Sites	Bypass
Bank-A	83	1	685	14	330	74
Bank-B	1,549	-	2,683	-	327	-
CreditCard	89	61	0	0	12	0
Trading-A	0	0	0	0	6	6
RideSharing	7	0	363	1*	1378	5*
WebInfrastructure	0	0	1	1	220	219

Reaction

- Clear writing, good explanations
- Concrete E2E attack on real services
- Well-engineered attack
- Analysis of ecosystem, trends

- Impact (only 16/300 sites affected)
- Moving target
  - Phishing and anti-phishing landscape changes quickly
- Realistic threat model?



Threat Model

- What parts of this threat model are realistic?
- What parts could stand to be improved?

Use of RBA / FP

- Is this even a good idea?
- Can we ask users to do 2FA more often?

Impact / Longevity

- Is use of FP to disable 2FA an upward trend? Passing phase?
- What about 2FA MITM?
- What about passkeys?
- What about anti-FP?

RBA and Privacy

- Anti-fraud techniques often conflict with privacy
  - IP tracking
  - Fingerprinting
  - Cookies
- How to balance privacy-invasive tech and anti-fraud benefits?