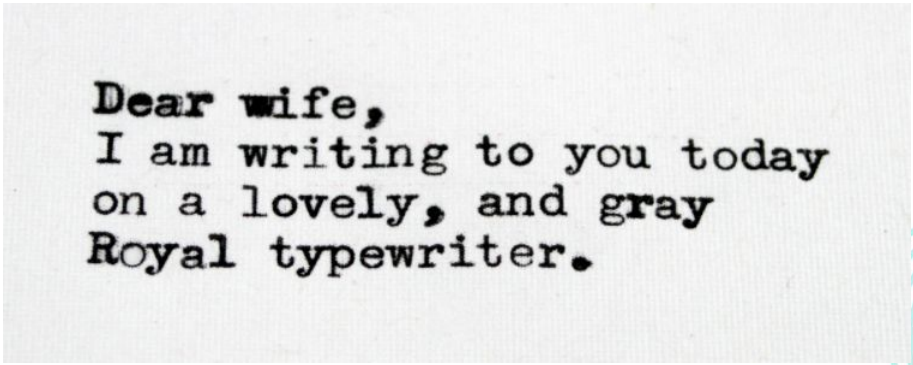
Browser Fingerprinting

študent: Peter Hraška
školiteľ: RNDr. Michal Forišek, PhD.

Čo je to fingerprinting?

- “žiadne dve zariadenia nie sú totožné”
- metóda autentifikácie
  - fotoaparát
  - písací stroj
  - web browser



Využitie browser fingerprintingu

- metóda identifikácie
- viacfaktorová autentifikácia
- obrana pred útokmi
- personalizovaný obsah
- reklama na mieru
- ...

Predošlé výsledky (1)

- Panopticlick (2010)
  - 470,161 vzoriek dát
  - 10 rôznych údajov
  - 18.1 bitov entropie (1 z 286,777)
  - Flash, Java
  - blokovanie napomáha identifikácii
- AmIUnique
  - 119,000 vzoriek dát
  - 17 rôznych údajov
  - prvý krát canvas fingerprint
- Browserprint

Predošlé výsledky (2) - smartphony

- Panopticlick
  - fingerprinty sú uniformnejšie
  - menší výber browserov
  - menej prvkov na prispôsobenie
  - absencia Flashu na iPhoneoch
- AmIUnique
  - väčšina údajov obsahuje na smartphoneoch menej entropie
  - user-agent stringy sú veľmi rôznorodé
  - 81% (spomedzi ~13,000) fingerprintov zo smartphoneov bolo unikátnych
- využitie senzorov na fingerprinting
  - iba so súhlasom používateľa

Náš cieľ

- state-of-the-art skript na zber fingerprintov
  - kombinácia existujúcich (Panopticlick, AmIUnique, Browserprint, fingerprint2js, ...)
  - doplnené o naše nápady a vylepšenia
- presnejšie dáta, nové výsledky
  - smartphony
  - implementácia v reálnej aplikácii
- implementácia v reálnych podmienkach
  - bez povšimnutia používateľa
  - nič, čo vyžaduje súhlas používateľa
  - nespomalí aplikáciu
  - Adobe v 2020 ukončí podporu pre Flash

Zbierané dáta (1) - http://fp.virpo.sk

- dokopy 31 rôznych údajov

- časové pásmo (-60)
- rozlíšenie obrazovky (2048*1079)
- hĺbka farebného spektra (24)
- user agent (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3 ...)
- podpora dotykových giest (0, false, false)
- local storage (true)
- session storage (true)

Zbierané dáta (2)

- formát zápisu času
- “01/01/1970, 01:00:00” vs. “01/01/1970, 01:00:00 AM”)

- Math.tanh(-1e300)
- -1.42144882387**47245** vs -1.42144882387

- HTTP Accept Language
- "sk-SK,sk;q=0.9,cs;q=0.8,en-US;q=0.7,en;q=0.6"
- "en-US,en;q=0.5"

Zbierané dáta (3)

Zoznam fontov (JS + CSS)

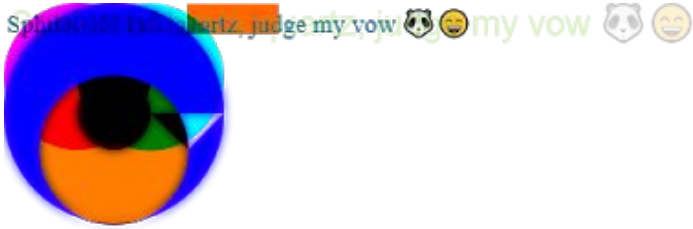
- ~60 rôznych fontov
- 3 záložné (fallback) fonty
- generovanie textu (3*60)
- porovnanie fontu oproti fallback fontu
- opravená chyba vo fingerprint2js

Zbierané dáta (4)

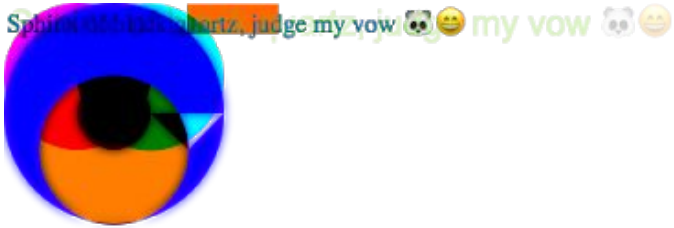
HTML5 Canvas fingerprint

- vyrenderujeme obrázok
  - transparentnosť
  - emoji
  - vynútenie fallback fontu
  - pangram
  - ...
- výsledkom je zahashovaná bitmapa

Windows



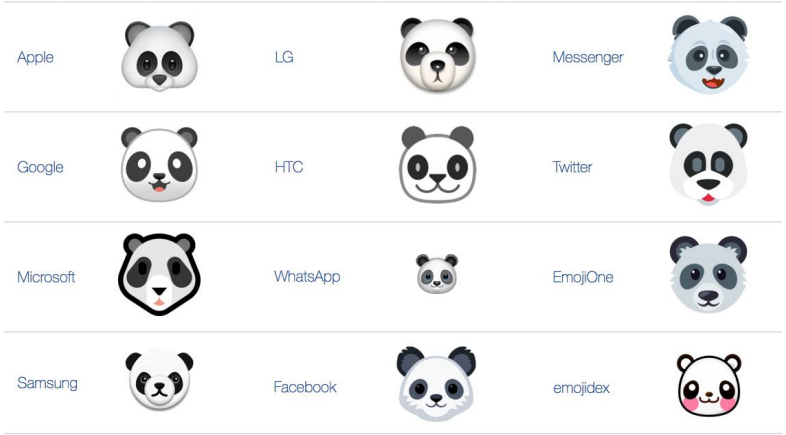
MacOS



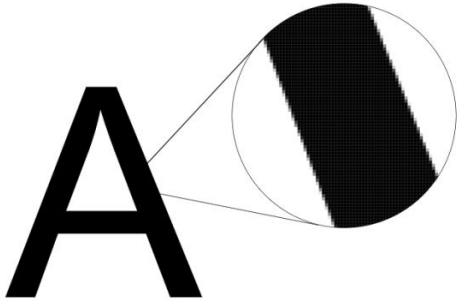
Zbierané dáta (5)

HTML5 Canvas - Prečo to funguje?

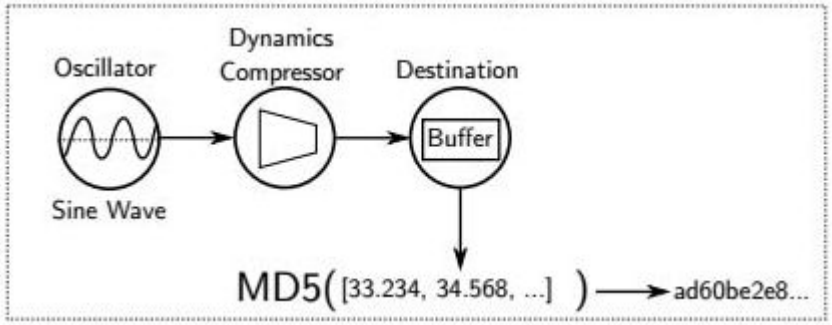
- fonty nie sú konzistentné
- emoji implementuje každý systém po svojom
- antialiasing



Arial 20px na 12 spôsobov

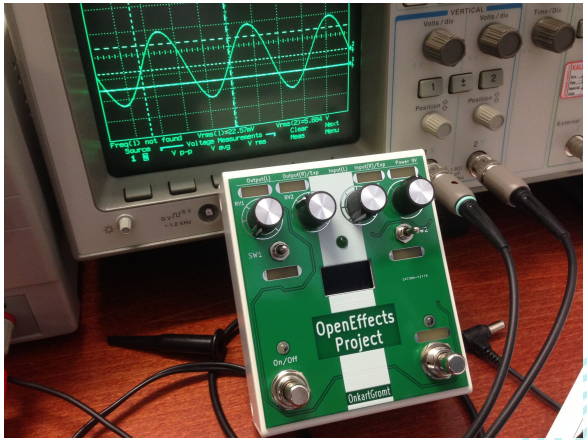


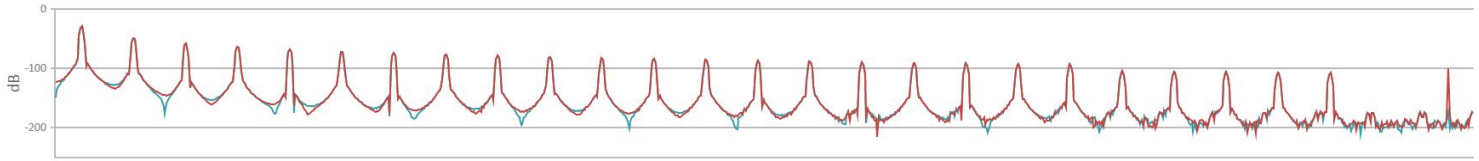
Zbierané dáta (6)



AudioContext

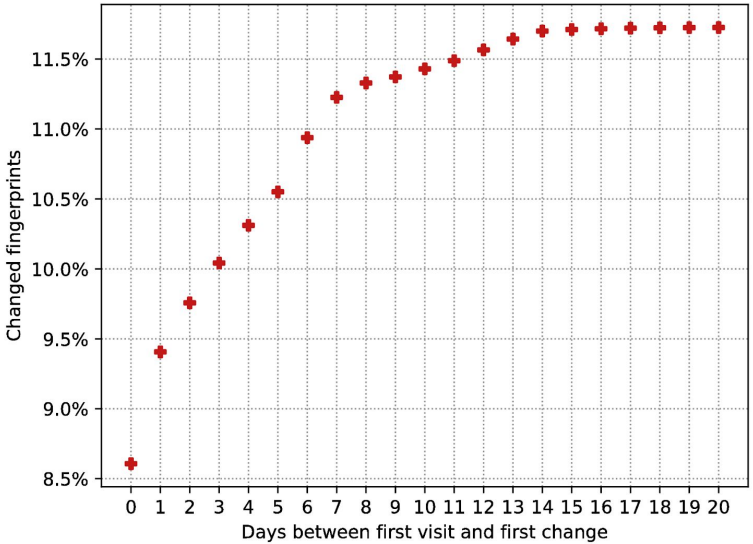
- súčasť Web Audio API
- generovanie zvukov, efektov, ... na webe
- AudioBuffer - zvuk uložený v číslach

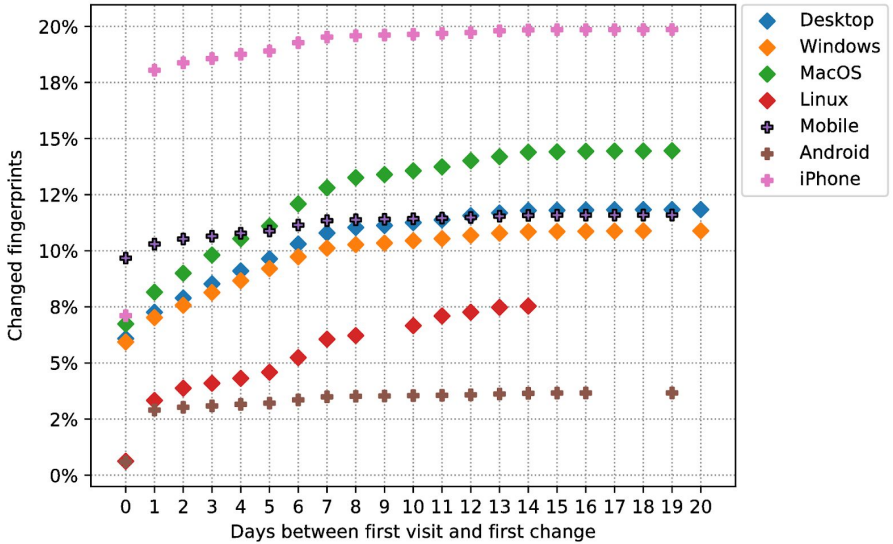




Zmena v čase

- Ako veľmi sú fingerprinty náchylné na zmeny?





(Ne)zbierané dáta

- Battery API
  - stav batérie
  - zostávajúca dĺžka nabíjania
  - z prehliadačov zmizne
- skok pri scrollovaní
- pohyb myšou
- posun času voči serveru

Alternatíva - supercookie, evercookie

Zámerne ťažko zmazateľné dáta

- HTTP Cookies
- Local shared object (Flash Cookie)
- Silverlight Isolated Storage
- Web history
- Local storage
- Session storage
- ...

- potreba zmazať všetky naraz
- inkognito ich schová

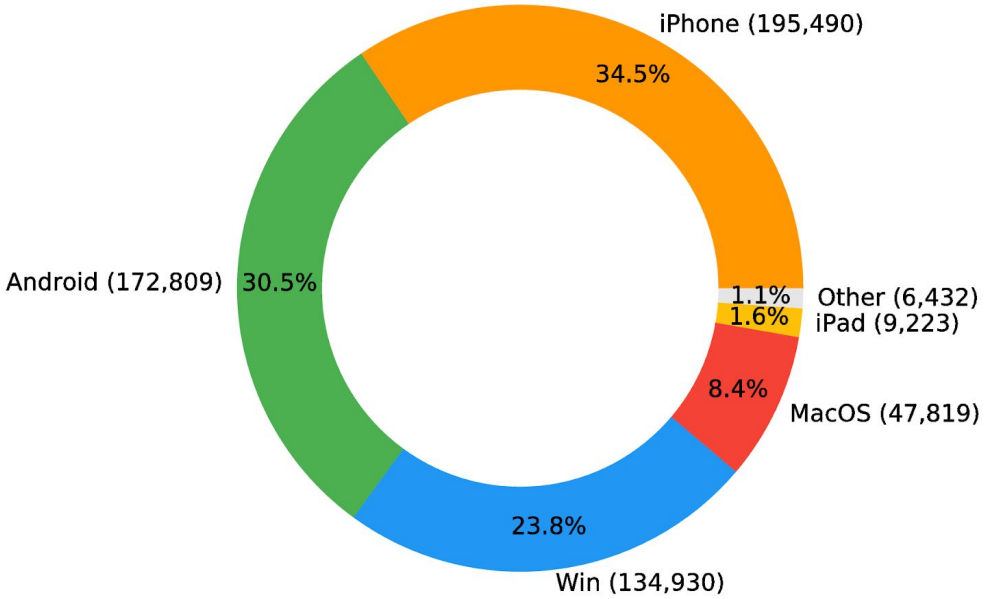
Naše výsledky (1)

- dáta z 3 zdrojov

- 355 fingerprintov - fp.virpo.sk
- 1,186 fingerprintov - malý web

- **566,704** fingerprintov na výslednú analýzu (65% z toho smartphony)
- 323,746 separátnych používateľov
- 177,677 (54.88%) z nich malo unikátny fingerprint

Naše výsledky (2)

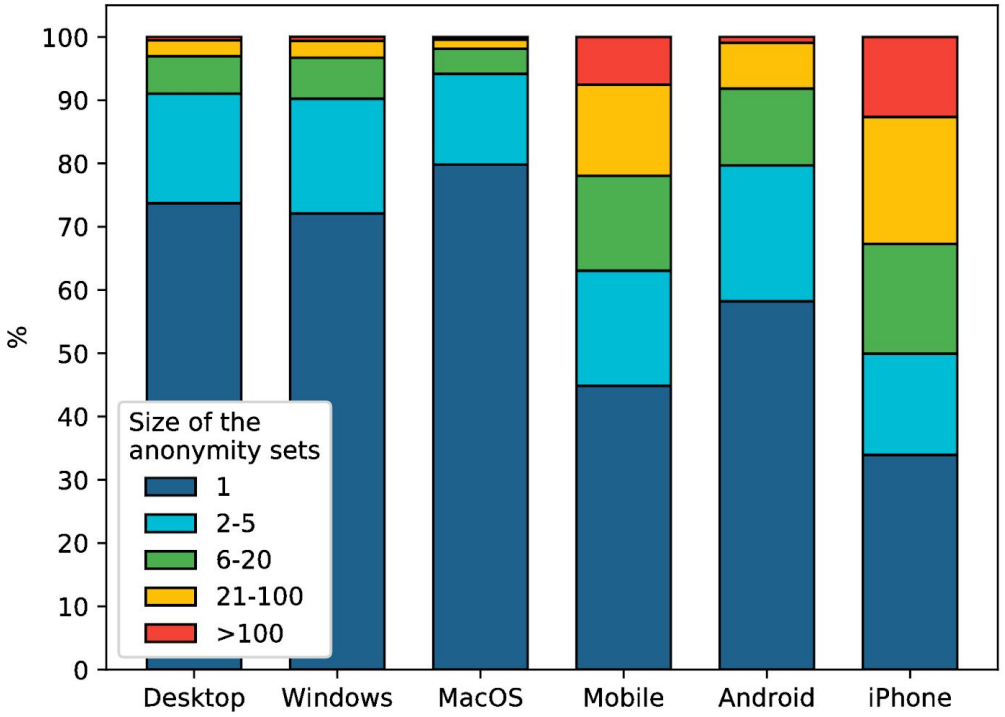


Naše výsledky (3)

- 16.685 bitov entropie
  - 1 z 105,362
- Panopticlick: 18.1
  - 1 z 286,777
- normalizovaná entropia:
  0.87 (my) vs 0.96 (Panopticlick)
- entropia v dátach z reálneho prostredia je nižšia, než doteraz namerané hodnoty

Naše výsledky (4)

-



Entropia pre rôzne zariadenia

	Desktop	Windows	MacOS	Linux	Mobile	Android	iPhone
All features	0.7818	0.7732	0.7627	0.7408	0.7589	0.7662	0.7225
JS features	0.7817	0.7731	0.7627	0.7409	0.7578	0.7638	0.7224
Headers	0.5131	0.4715	0.5151	0.5954	0.5898	0.7279	0.4274
AdBlock	0.0527	0.0467	0.0294	0.0217	0.0461	0.0545	0.0548
Audio FP	0.1144	0.0808	0.0398	0.0271	0.1480	0.0879	0.0890
Available size	0.1854	0.1255	0.0688	0.0255	0.1710	0.0993	0.1010

- silné na identifikáciu smartphoneov:
  - systémové jazyky, user-agent string, canvas, formát času
- slabé:
  - fonty, pluginy, math tanh

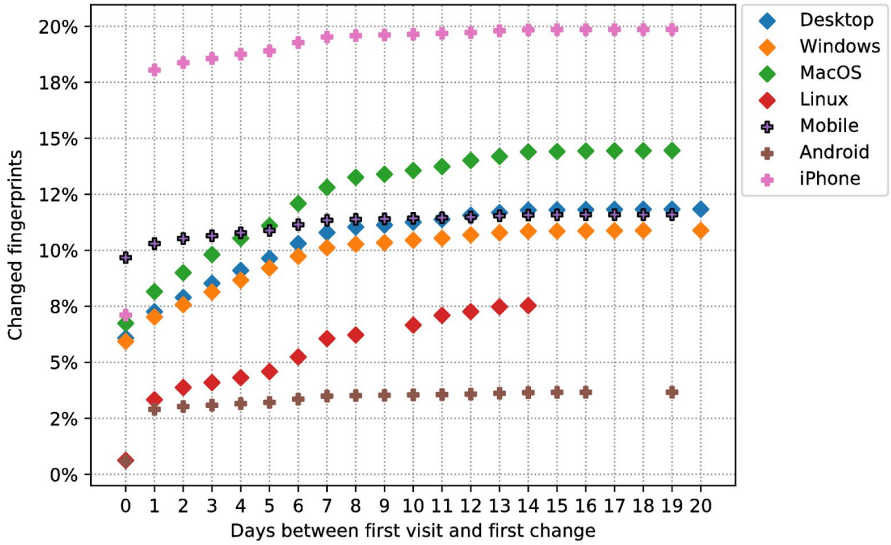
Minimálny fingerprint

- najlepší subset s obmedzením počtu údajov
- 12 odstránených = strata 0.003 bitov entropie

Subset size	Features	Entropy
3	Date format, User-agent, Available size	14.2218
4	All of the above + Canvas FP	15.2366
5	All of the above + WebGL renderer	15.7247
7	All of the above + DNT + HTTP language	16.3192
9	All of the above + Audio FP + Installed fonts	16.5168

Nestabilné parametre

- iPhone
  - canvas
  - audio
  - user-agent string
- Android
  - systémové jazyky
  - canvas
- Windows, MacOS
  - parametre displeja (screen size, available size, pixel ratio)
- update browsera mení user-agent string



Prevencia

- blokovanie je kontraproduktívne
- časté hodnoty - regulárny fingerprint
- “randomizácia” hodnôt
  - canvas
  - audio
- silu majú vývojári
  - Firefox
  - Apple (WWDC 4. jún 2018)
- GDPR
  - IP adresa a im podobné = osobný údaj

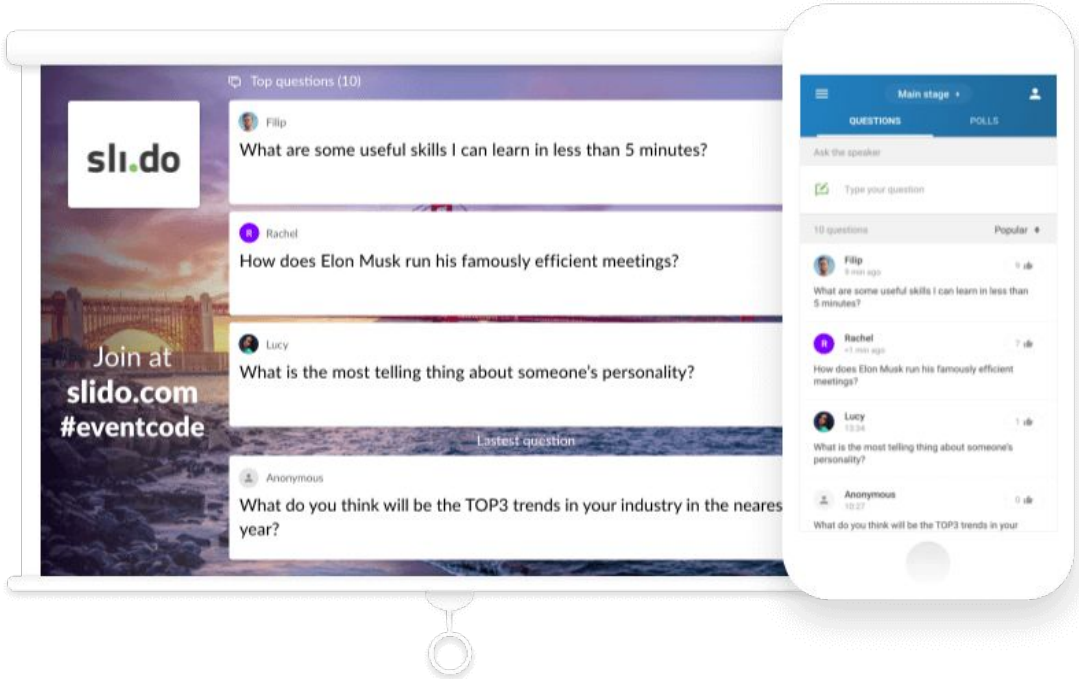
Zhrnutie

- 566,704 fingerprintov s 31 rôznymi údajmi
  - doteraz najväčší skúmaný dataset
  - z prostredia reálnych webových aplikácií
- 16.685 bitov entropie
  - menej, než v predošlých výskumoch
- 368,299 fingerprintov zo smartphoneov
  - prvá veľká analýza fingerprintov na smartphoneoch
- iba tretina iPhone zariadení má unikátny fingerprint
- prvá analýza, ktorá zahŕňa audio fingerprint
- formát dátumu, rozlíšenie (availSize) a user agent sú najsilnejšie
- súkromie majú v rukách vývojári

Ďakujem za pozornosť

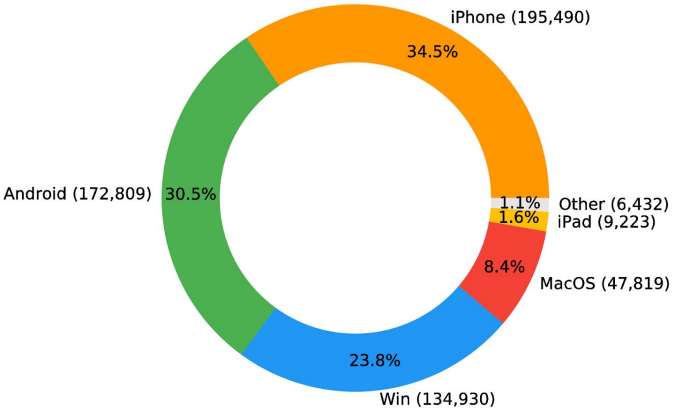
https://panopticlick.eff.org/static/browser-uniqueness.pdf
https://hal.inria.fr/hal-01285470/file/beauty-sp16.pdf (AmIUnique)
https://github.com/Valve/fingerprintjs2/
https://audiofingerprint.openwpm.com/

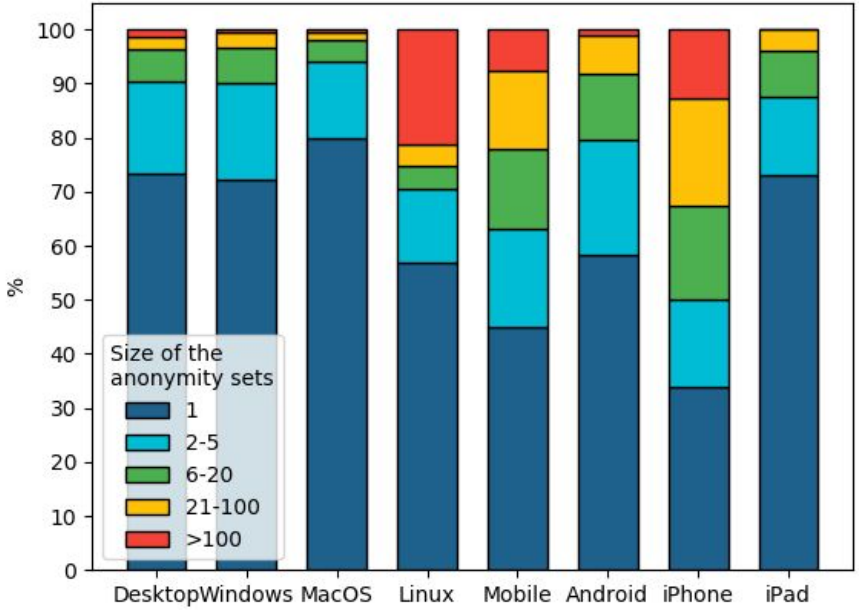
Primárny zdroj pre dáta - Slido



Linux

- menej než 1% dát
- automatizované testy
- malá signifikantnosť





Entropia pre rôzne zariadenia

- normalizovaná entropia

	Desktop	Windows	MacOS	Linux	Mobile	Android	iPhone
All features	0.7818	0.7732	0.7627	0.7408	0.7589	0.7662	0.7225
JS features	0.7817	0.7731	0.7627	0.7409	0.7578	0.7638	0.7224
Headers	0.5131	0.4715	0.5151	0.5954	0.5898	0.7279	0.4274
AdBlock	0.0527	0.0467	0.0294	0.0217	0.0461	0.0545	0.0548
Audio FP	0.1144	0.0808	0.0398	0.0271	0.1480	0.0879	0.0890
Available size	0.1854	0.1255	0.0688	0.0255	0.1710	0.0993	0.1010

...

Veľkosť okna na desktope

- dvojsečná zbraň
  - v TOP 3 pre entropiu
  - v TOP 3 pre nestabilné parametre
- meniť sa dá veľa parametrov, analyzovali sme všetky
- implementáciu treba šiť na mieru
- Facebook a spol. využívajú canvas
  - prístupná miera nestability

Minimálny fingerprint a čas

- MacBook Pro 2016, OnePlus 3, Nexus 6 (Motorola)

			Time [ms]		
#	Features	Entropy	MBP	OP3	Nexus 6
3	Date format, User-agent, Available size	14.222	1	10	9
4	+ Canvas FP	15.237	24	89	124
5	+ WebGL renderer	15.727	35	101	164
7	+ DNT + HTTP language	16.319	35	108	167
9	+ Audio FP + Installed fonts	16.517	62	154	310
31	All	16.685	74	175	334