

Device Fingerprinting alebo Hardwarometria vs. Biometria

*e*FOCUS

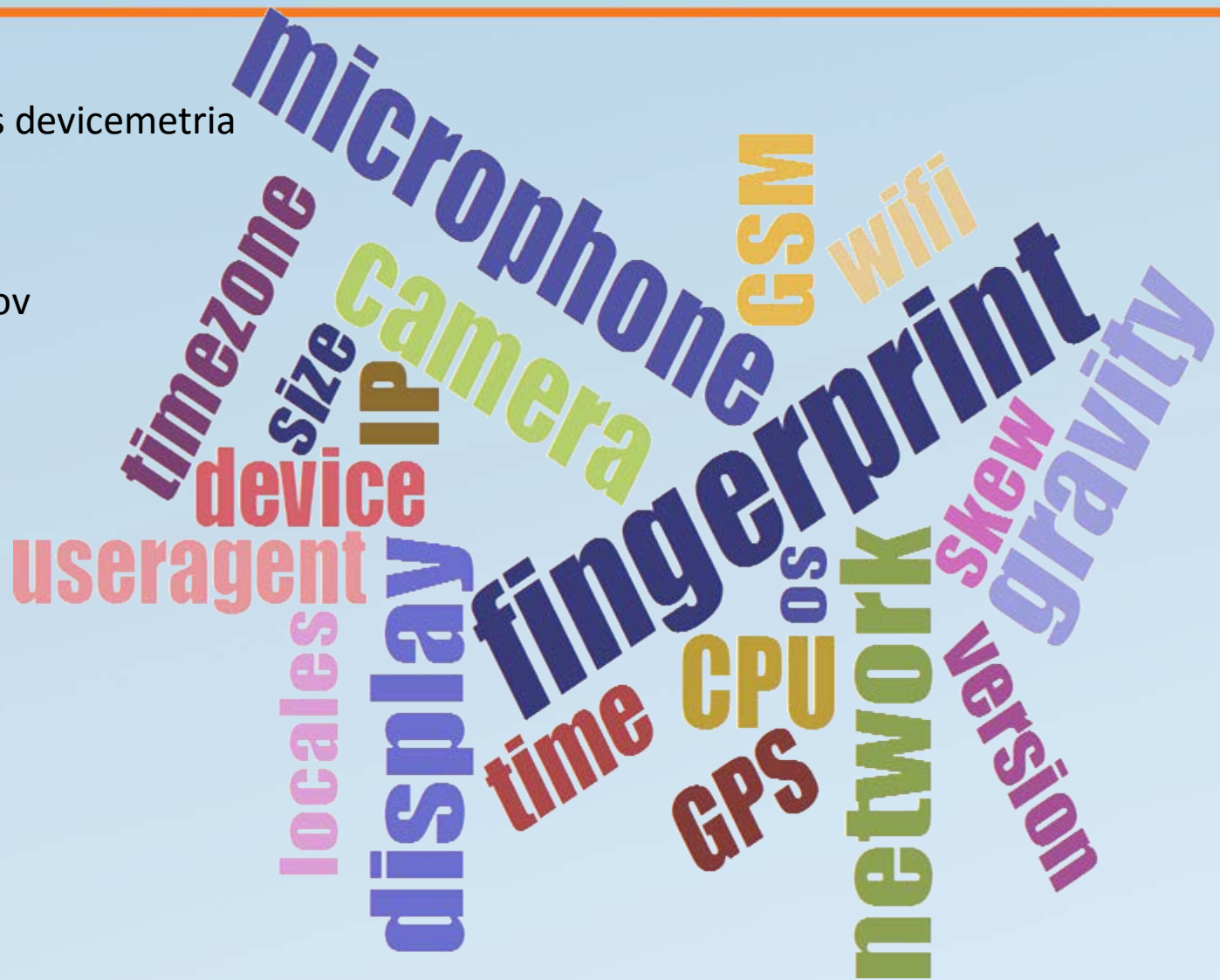


TATRA BANKA

Member of Raiffeisen Bank International

Agenda

- Biometria vs devicemetria
- Použitie
- Rozdelenie
- Prehľad typov
- Záver



Biometria vs devicemetria

- Biometria je založená na meraní biologickej alebo fyziologickej vlastnosti ľudského tela
- Biometrické identifikátory sú odlišiteľné, merateľné charakteristiky použité na označenie individuálnej osoby
- **Jedinečnosť** – žiadne dve osoby by nemali mať rovnaké charakteristiky v zmysle merania a porovnávanej skupiny.
- **Univerzalita** – danou charakteristikou by mala disponovať každá osoba v skupine
- **Stálosť** – charakteristika osoby by sa v čase nemala meniť alebo meniť veľmi pozvoľna
- **Merateľnosť** – veľmi dôležitá vlastnosť pre automatizované systémy – reprezentuje rýchlosť, jednoduchosť a opakovateľnosť merania
- **Výkonnosť** – presnosť identifikácie
- **Prijateľnosť** – miera ochoty používať daný systém osobami
- **Bezpečnosť** – odolnosť voči podvodným technikám
- **Cena** – posledná charakteristika je ekonomickým parametrom miery nasadenia systému.

Biometria vs devicemetria

- Odtlačok zariadenia alebo odtlačok stroja sú informácie zhromaždené o vzdialenom výpočtovom zariadení na účely jeho identifikácie. Odtlačky môžu byť použité na úplnú alebo čiastočnú identifikáciu jednotlivých užívateľov alebo zariadení.
- **Rozmanitosť** - žiadne dve zariadenia nemajú rovnaký fingerprint.
 - veľké množstvo zariadení má rovnaké konfiguračné nastavenie, a teda pravdepodobne rovnaký fingerprint.
- **Stabilita** - fingerprinty zostávajú rovnaké v čase.
 - konfigurácie zariadení sa môžu ľubovoľne modifikovať.
 - riešenie je znížiť počet parametrov, merať iba tie, ktoré sú málo náchylné na zmeny
 - znižuje rozmanitosť

Tradičný prístup

- UDID
- IDFA
 - Nepovolené pre aplikácie nezobrazujúce reklamy
- môžu sa zakázať
- premenlivé v čase



EFF ELECTRONIC FRONTIER FOUNDATION DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD							
HOME	ABOUT	OUR WORK	DEEPLINKS BLOG	PRESS ROOM	TAKE ACTION		
Who Has Your Back?							
PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS							
	Follows industry-accepted best practices	Tells users about government data demands	Discloses policies on data retention	Discloses government content removal requests	Pro-user public policy: opposes backdoors		
Adobe	★	★	★	★	★		
amazon.com	★	★	★	★	★		
Apple	★	★	★	★	★		
at&t	★	★	★	N/A	★		

Sensory – prehľad typov

- CPU
- Kamera
- Mikrofón
- Gyroskop
- Kompas
- Magnetometer
- Akcelerometer
- Dotykový displej
- Hodiny
- GSM
- GPS
- Sieť
- Wifi

CPU - MESC

- **Machine Effective Speed Calibration**
- meria sa čas transakcie na zariadení
- rovnaký program beží na dvoch rovnakých zariadeniach, ale v dôsledku okolností (obsadenie pamäte, vyťaženie CPU) sa čas bude líšiť pre každé zariadenie v porovnaní s ostatnými zariadeniami

CPU – MESC

US 20140181488 A1

```
function CalculateMESC( )
{
    var calibration_time = 1000; //One second. (in milliseconds)
    var num_of_iterations = 0;
    var currentTime = (new Date( )).getTime( ); //Get the start time ((in
    milliseconds)

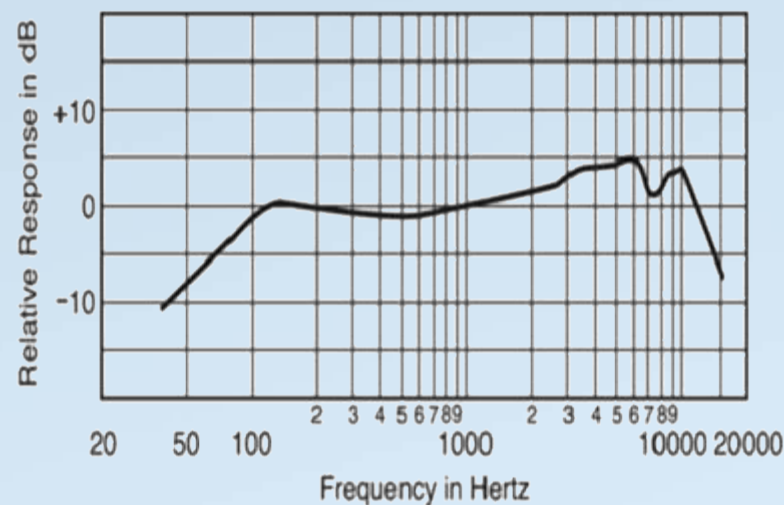
    //Calculate the end time (in milliseconds) at which the calibration will be
    stopped.

    var endTime = (new Date( )).getTime( ) + calibration_time;
    while (currentTime < endTime)
    {
        num_of_iterations++;
        currentTime = (new Date( )).getTime( );
    }
    return num_of_iterations;

} //end of function CalculateMESC
```

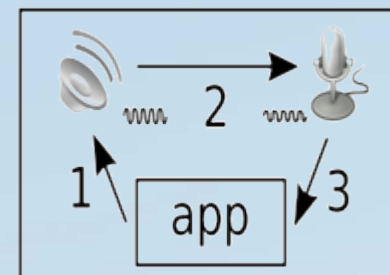
Mikrofón

- **Reproduktor - mikrofón systém**
- Systém používa reproduktor na vysielanie zvuku s rôznymi frekvenciami a nahráva ho prostredníctvom mikrofónu. Odlačkom je skreslenie signálu medzi skutočnou amplitúdou-frekvenciu a vysielanou.
- V dôsledku výrobných odchýlok sú frekvenčné odozvy odlišné pre každý mikrofón alebo reproduktor aj keď sú určené pre rovnaký model zariadenie
- Typická krivka frekvenčnej odozvy mikrofónu.
- Všimnite si, že pre niektoré frekvencie zvuku je mikrofón
- citlivejší (viac ako 0 dB) kým pre iné frekvencie utlmený (menšie než 0 dB)

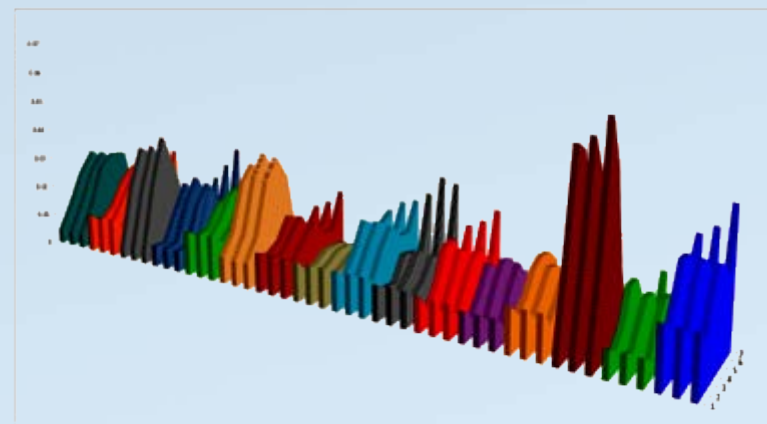


Mikrofón

- Schéma analýzy zvukovej spätnej väzby. V medziach zariadení, aplikácia vysiela zvuk prostredníctvom vstavaného reproduktora (1),
- zvuk dosiahne mikrofón v skreslenej a oslabenej forme (2), a aplikácia zaznamenáva signál mikrofónu a analyzuje ho (3).



- meranie pomeru spätnej väzby pre niekoľko rôznych frekvencií
- zariadenie musí byť v relatívne pokojnom prostredí
- Porovnanie druhej-harmonickej krivky na rôznych zariadeniach. Každý prístroj je zastúpený tromi susednými krivkami, ktoré majú rovnakú farbu.



Akcelerometer

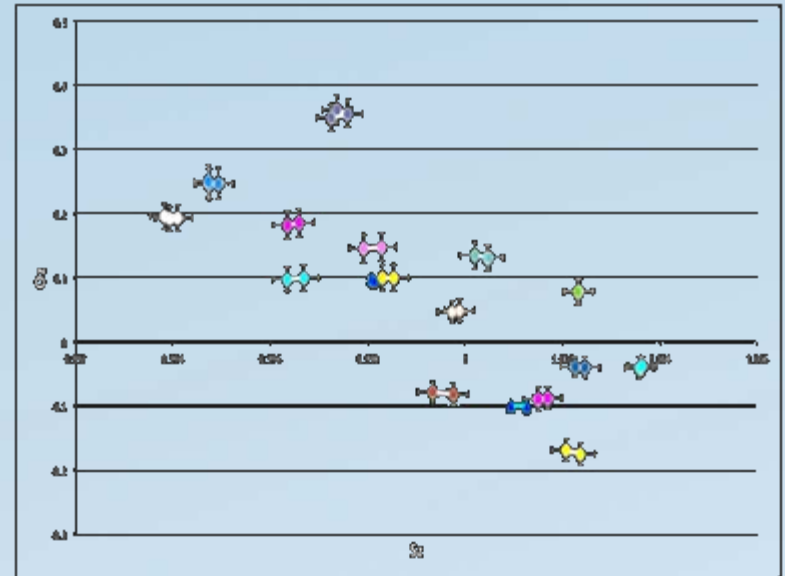
- Akcelerometer meria zrýchle zariadenia vo všetkých 3 osiach.
- Meranie v_m je vo vzťahu k skutočnému zrýchleniu zariadenie v_t vyjadrené rovnicou:

$$v_m = v_t S_v + O_v$$

S_v a O_v sú parametre reprezentujúce citlivosť a posun akcelerometra

- 3D senzory majú 6 parametrov.

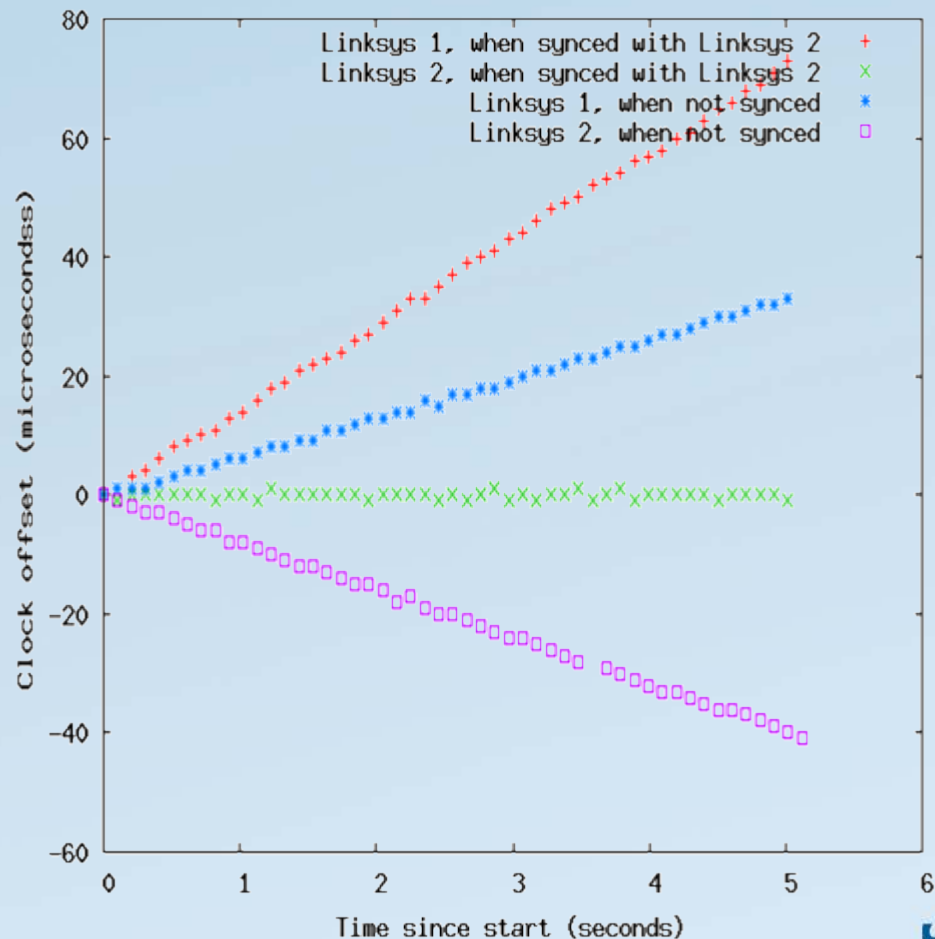
```
window.ondvicemotion = function(event) {  
    var x = event.accelerationIncludingGravity.x;  
    var y = event.accelerationIncludingGravity.y;  
    var z = event.accelerationIncludingGravity.z;  
    ...  
}
```



Bodový diagram dát získaných pomocou akcelerometra zo 17 zariadení so systémom iOS

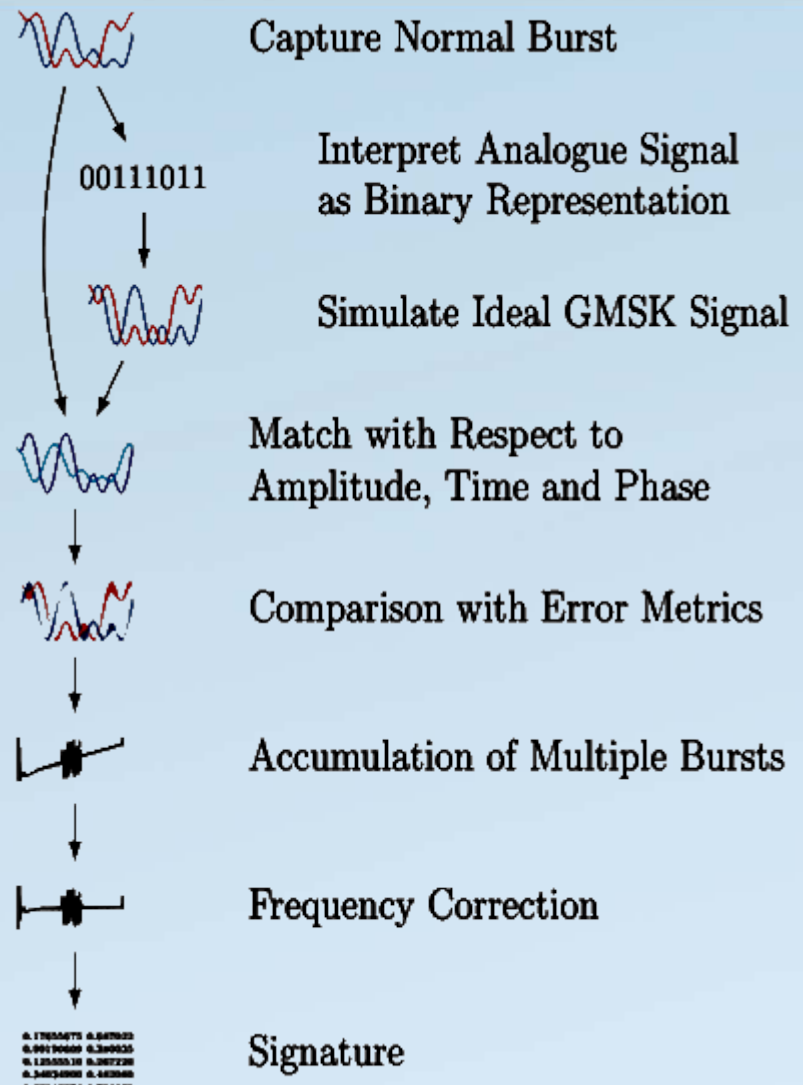
Skreslenie hodín

- Založené na meraní časových identifikátorov v TCP a ICMP paketocho
- Každé zariadenie má vlastný oscilátor generujúci časový signál
- V dôsledku výrobných odchýlok sa oscilátori líšia v presnosti
- - krátkodobá stabilita



GSM

- Založené na meraní odlišnosti modulácie skutočného signálu voči ideálnemu
- dlhodobá stabilita
- dostupné len operátorom
- vhodné pre forenznú identifikáciu



SW

- Zbieranie príznakov z celého dostupného ekosystému zariadenia
 - verzia OS
 - rozlíšenie displeja
 - user_agent
 - lokalizácia (SK, EN ...)
 - časová zóna
 - iné nainštalované aplikácie
 - fonty
 - canvas
- Možnosť cielenej zmeny



Firefox 24 (hore) Chromium 35 (dole)

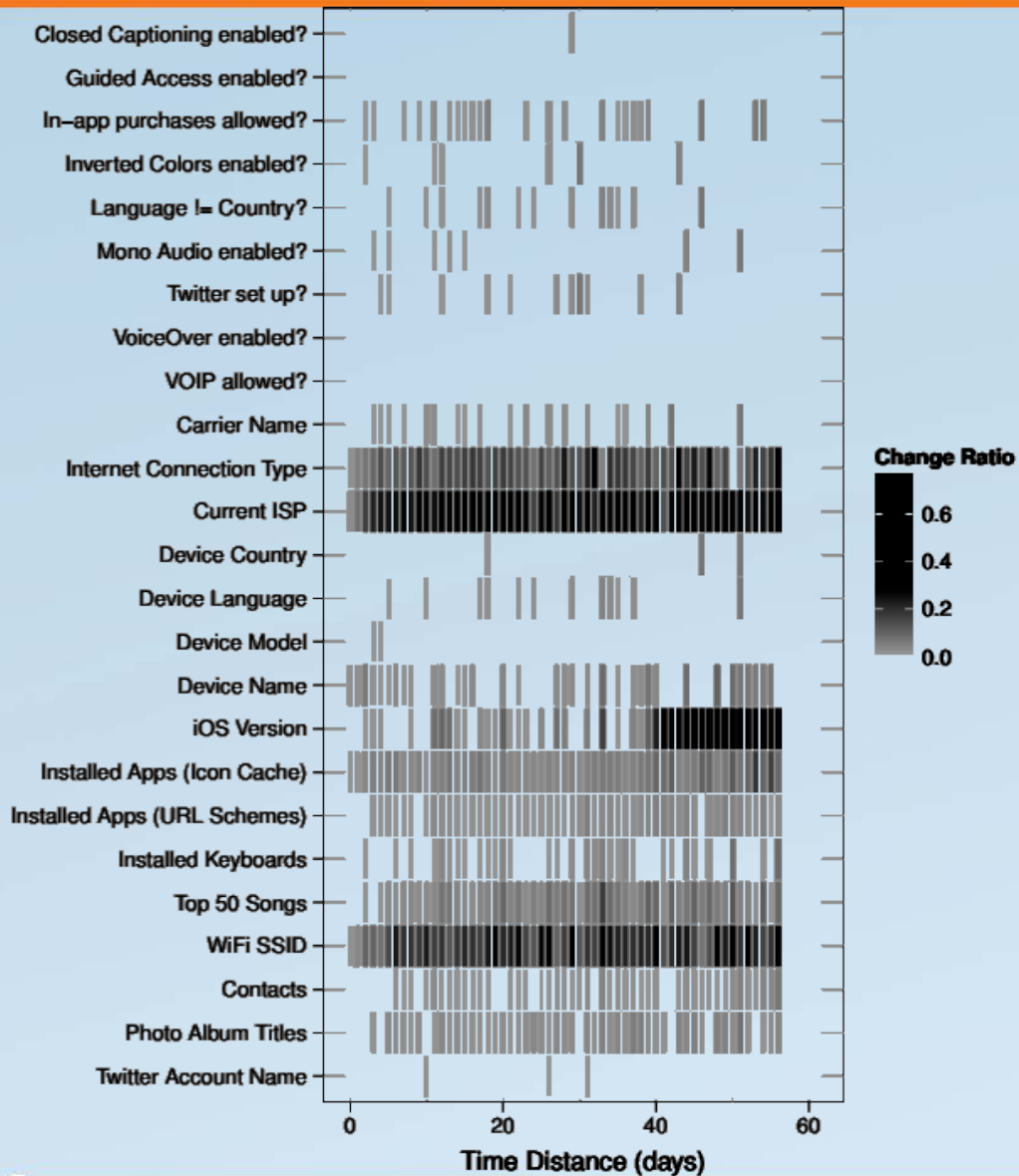
Your computer drew this fingerprint image:



...which can be turned into an ID code like:

661c99f0bb03a7b785e6ea3b0deb7a37

SW



Záver

- Spolu s nárastom príjmov z e-commerce, narastá rovnako záujem o jeho zneužitie.
- Fyzická neprítomnosť + anonymizácia klienta počas transakcie/loginu vyžaduje alternatívu pri verifikácii
- Zariadenie už nie je prideľované (483/2001 Z. z. § 89 ods. 3), ale vo vlastníctve zákazníka (BYOD)
- Fingerprinting nie je všeliek, ale významne môže napomôcť
- V rozpore so stratégiou ochrany súkromia zo strany výrobcov smartphonov

Ďakujeme za pozornosť

