FP-Block

Usable web privacy via fingerprint

Hugo Jonker

Open Universiteit
www.ou.nl

Joint work with Sjouke Mauw (UL), Christof Ferreira Torres (UL)

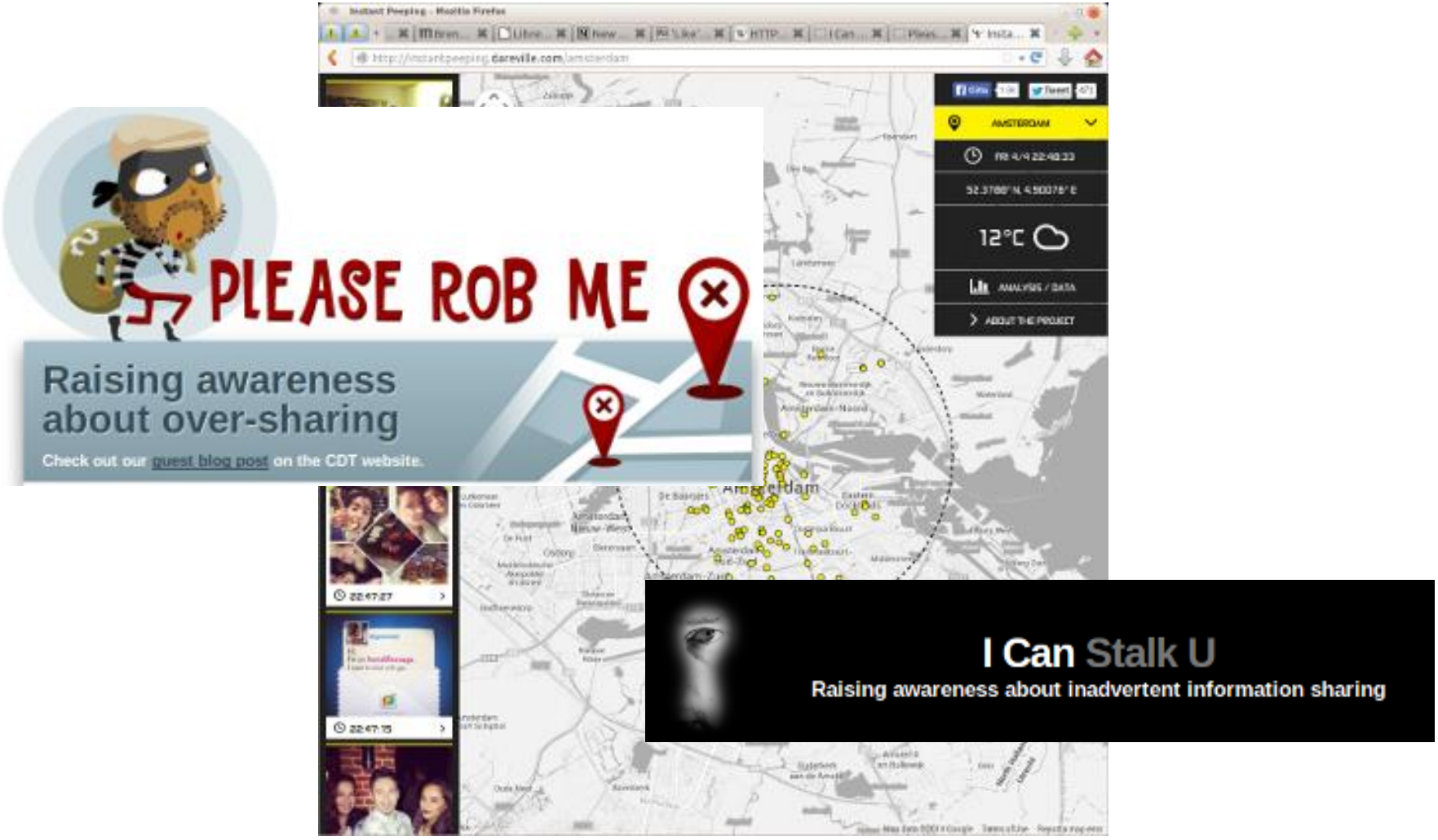
First

Privacy does not need to be motivated.

Violation of privacy needs to be motivated.

see also *Je hebt wél iets te verbergen - Maurits Martijn & Dimitri Tokmetzis*
https://kiosk.decorrespondent.nl/products/je-hebt-wel-iets-te-verbergen-boek

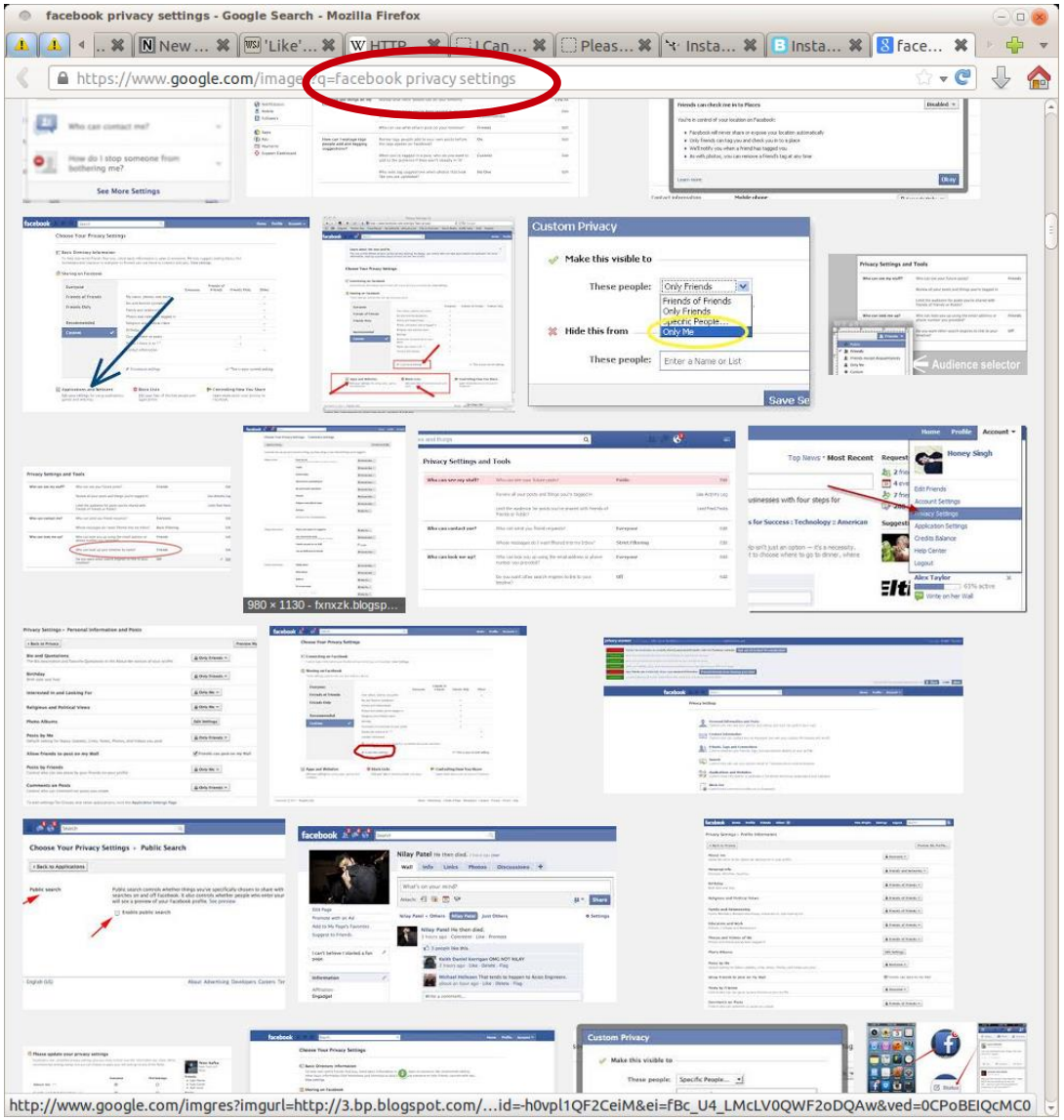
We're not really good at privacy



We're **really** not good at privacy

Note: account number can suffice for withdrawal

Privacy is hard



Privacy is **really** hard

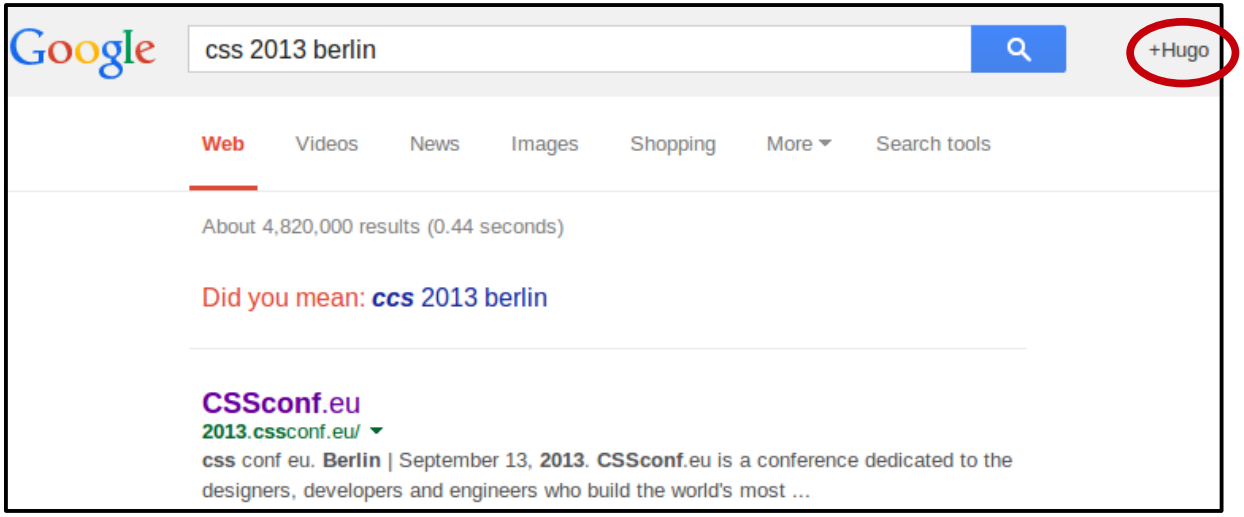
*"Another thing which is just an observation, when I was working on the **blocking of the social plugins**, I always used the [redacted] website to test my implementation. Today **Facebook suggested** me on my phone the **group of** [redacted]."*

– Bachelor student

Privacy is **really really** hard

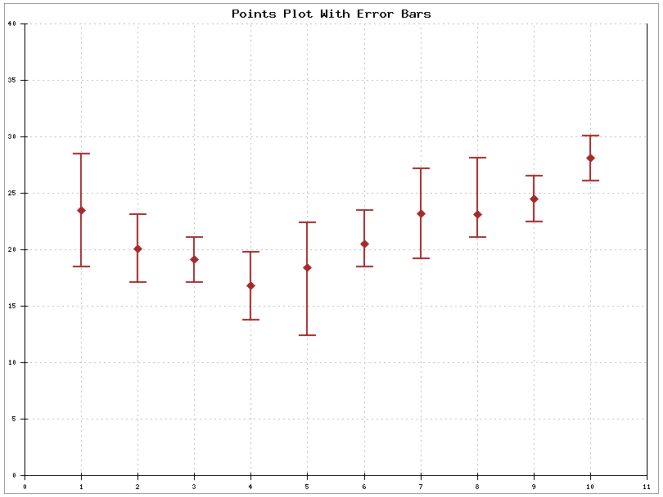
TECH | 2/16/2012 @ 11:02AM | 2,398,698 views

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



Actually, what is privacy?

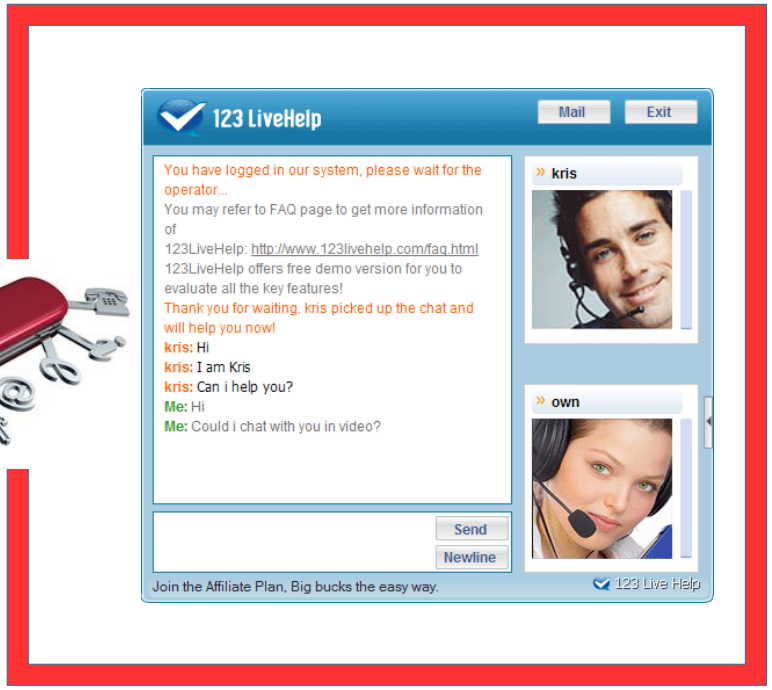
- Privacy is secrecy wrt. someone
- Two aspects:
  - (in)distinguishability
  - (un)certainty



Did privacy become harder?

In a nutshell

≈



Contributions

- New paradigm for online privacy
- Distinguish between local and cross-domain tracking
- Fingerprint privacy via separating web identities
- Determined common fingerprint vectors

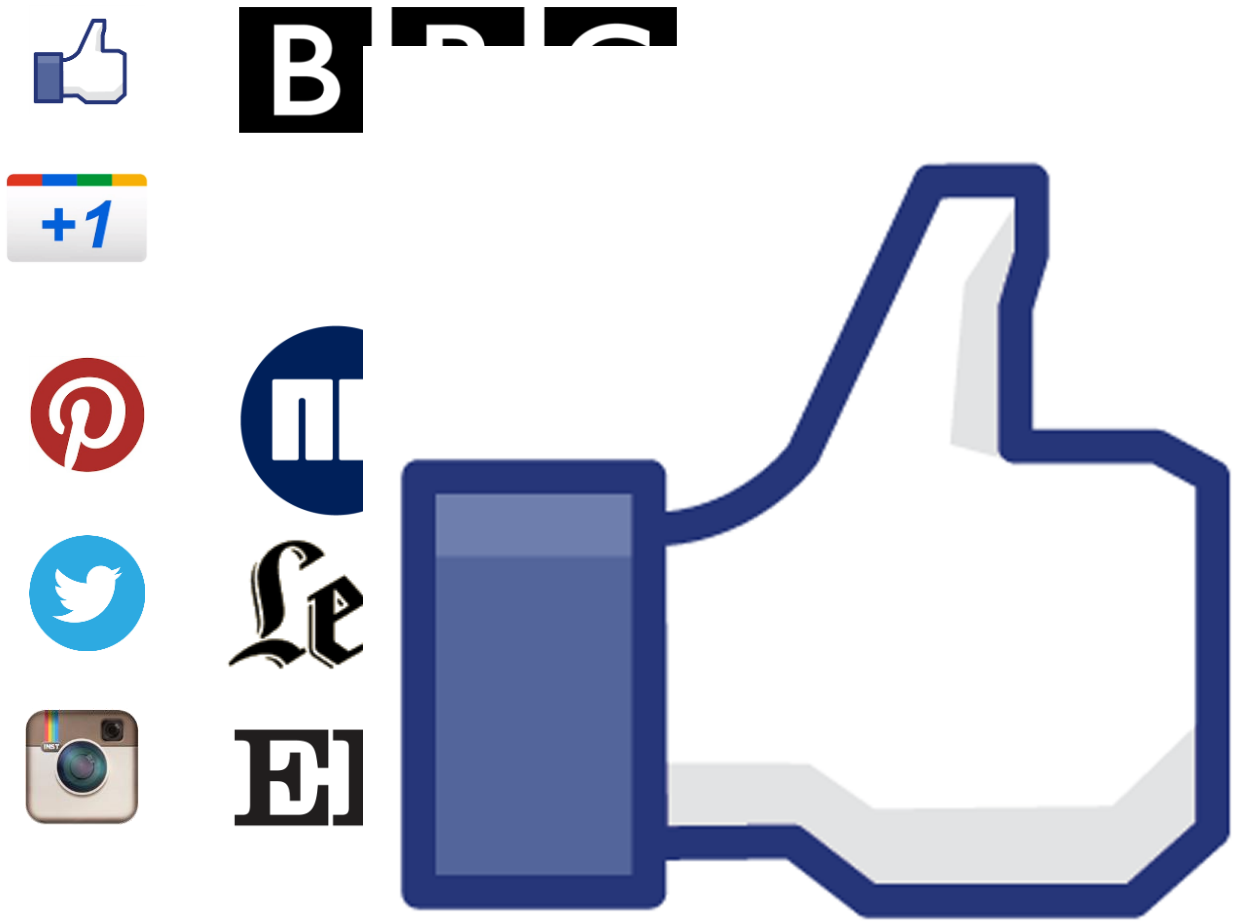
- Proof-of-concept implementation
  - https://github.com/ChristofTorres/FP-Block
  - effective against commercial fingerprinters

Web tracking

Tracking is good!

- Fraud prevention
- Improving web site usability
  - Finding common browsing “errors”
  - Related items of interest
  - ...

However...



Embedded content

1. Content delivery networks
2. Advertising
3. Analytics and tracking
4. Embedded media
5. Social plugins
6. Payment
7. Libraries
8. ….

		Top 10k
1.Akamai		17%
2.Doubleclick		10%
3.Google Analytics	19%	
4.YouTube		26%
5.Facebook Like*	20%	
6.PayPal button		33%
7.JQuery		18%

* aggregated numbers from builtwith.com.
Numbers by similartech.com are higher.

Open Universiteit
www.ou.nl

How to track

- Client-side
  - Cookies / evercookies / zombiecookies / ...
  - History exploit / CSS tricks / ...
  - Active fingerprinting

- Server-side only
  - Web bugs
  - Passive fingerprinting

Why fingerprinting?

- Cookies: client-side storage.
- Fingerprinting:
  - Passive: infer info from server side.
  - Active: gather info from client side on-the-fly.

- Effective?
  - [PETS10]: 90% desktop browsers is unique.
- Actually in use?
  - [S&P13, CCS13]: some, but not much... yet.
  - **Firefox 42 Beta added “tracking protection”**

Effectiveness of fingerprinting [PETS10]

- 90% of desktop browsers unique
- No JS ⟶ better results
- Mobile ⟶ less plugins ⟶ better results

- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)

- Revealing: order of fonts, order of plugins
- Defensive paradox

Fighting fingerprinting

- Do Not Track header? [NSDI12]: **X**
- Blacklisting fingerprinters? [W2SP11]: **X**

- FireGloves [NordSec11]? [CCS13]: **X**
- Tor Browser? [CCS13]: **X**

Any countermeasure can be broken if specifically targetted.

Idea:

- local tracking okay,
- 3rd party tracking not

Open Universiteit
www.ou.nl

Lots of ways to fingerprint

E.g.

- [PETS10] – User-agent
- [W2SP11] – fingerprinting JavaScript implementations
- [W2SP12] – fingerprinting HTML5 font rendering
- [W2SP13] – fingerprinting JS engine errors
- TCP/IP clock skew can be passively detected (proxies don't help)
- HTTP header order
- ...

“Fingerprint surface”

Non-profit:

- Panopticlick - academic study
- FingerPrintJS - open source

Commercial:

- AddThis - social media buttons
- BlueCava - advertisements [S&P13]
- Iovation - fraud prevention [S&P13]
- ThreatMetrix - fraud prevention [S&P13]

Fingerprint vectors [S&P13]

- Plugin Enumeration
- Font Detection
- User-Agent
- HTTP Header Accept
- HTTP Header Accept-Charset
- HTTP Header Accept-Encoding
- HTTP Header Accept-Language

- Java Enabled
- DNT User Choice
- Cookies Enabled
- Flash Enabled
- ActiveX + CLSIDs
- Date & Time
- CPU
- System/User Language
- OpenDatabase
- Canvas Fingerprinting
- Mime-type Enumeration
- HTTP Proxy Detection
- IndexedDB
- Math Constants

- Windows Registry
- TCP/IP Parameters
- Google Gears Detection
- Flash Manufacturer
- MSIE Security Policy
- AJAX Implementation
- MSIE Product key
- Device Enumeration
- Device Identifiers
- IP address
- HTML Body Behavior
- Battery
- WebGLRenderingContext

static

IE specific

using DLL

Fingerprint vectors

- √: this work
- √: [S&P13]
- –: [S&P13], but dropped

Attribute	Pan	BC	IO	TM	Add	FPjs
Plugin Enumeration	✓	✓	✔	✓	✔	✔
Font Detection	✓	✓		✓		
User-Agent	✓	✓	✓	✓	✔	✔
HTTP Header Accept	✓					
HTTP Header Accept-Charset	✓					
HTTP Header Accept-Encoding	✓					
HTTP Header Accept-Language	✓					
Screen Resolution	✓	✓	✓	✓	✔	✔
Timezone	✓	✓	✓	✓	✔	✔
Browser Language		✓	✓	–	✔	✔
OS & Kernel Version		✔	✔	✓	✔	✔
DOM Storage	✓	✔	✔	✔	✔	✔
IE userData	✓	✔				
Java Enabled	✔				✔	
DNT User Choice		–			✔	✔
Cookies Enabled	✓		✔			
JS detect: Flash Enabled	✓	✓	✓	✓	✔	✔
ActiveX + CLSIDs	✓	✓		✓	✔	✔
Date & Time		✔	✓	✔	✔	
CPU		✔	✔		✔	✔
System/User Language		✓	✔		✔	
OpenDatabase			✔		✔	✔
Canvas Fingerprinting					✔	✔
Mime-type Enumeration	✓			✓		
HTTP Proxy Detection			✓	✓		
IndexedDB					✔	✔
Math Constants		✓			✔	
Windows Registry		✓	✓			
TCP/IP Parameters		✓	✓			
Google Gears Detection		✓				
Flash Manufacturer				✓		
MSIE Security Policy		✓				
AJAX Implementation		✓				
MSIE Product key			✓			
Device Enumeration		✓				
Device Identifiers			✓			
IP address		✓				
HTML Body Behavior						✔
Battery					✔	
WebGLRenderingContext					✔	

Proof-of-concept: FP-Block plugin

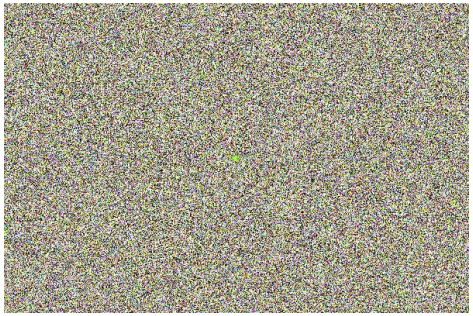
- Generates consistent fingerprint
- One fingerprint per primary domain
- 23 attributes (Tor: 14, FireGloves: 8)
- Covers
  - HTTP (passive fingerprinting)
  - JavaScript (active fingerprinting)
- Additional coverage to ensure functionality
- Canvas fingerprint
  - detection [CCS14]
  - prevention (new)

FP-Block's fingerprint coverage

Original canvas

+

+



Attribute	FG	Tor	PV	RAS	FPB
Plugin Enumeration	✔	✔	✔		✔
Font Detection	✔	✔	✔	✔	✔
User-Agent	✔	✔		✔	✔
HTTP Header Accept					
HTTP Header Accept-Charset		✔			
HTTP Header Accept-Encoding				✔	✔
HTTP Header Accept-Language		✔		✔	✔
Screen Resolution	✔	✔		✔	✔
Timezone	✔	✔		✔	✔
Browser Language	✔				✔
OS & Kernel Version	✔	✔		✔	✔
DOM Storage				✔	✔
IE userData					
Java Enabled					✔
DNT User Choice				✔	✔
Cookies Enabled					✔
JS detect: Flash Enabled					✔
ActiveX + CLSIDs					
Date & Time					
CPU				✔	✔
System/User Language					✔
OpenDatabase					✔
Canvas Fingerprinting		✔		✔	✔
Mime-type Enumeration	✔	✔	✔		✔
HTTP Proxy Detection					
IndexedDB					✔
Math Constants					
Windows Registry					
TCP/IP Parameters		✔			
Google Gears Detection					
Flash Manufacturer					
MSIE Security Policy					
AJAX Implementation					
MSIE Product key					
Device Enumeration					
Device Identifiers					
IP address		✔			
HTML Body Behavior					
Battery		✔			✔
WebGLRenderingContext		✔		✔	✔

Validation

- Verify setup
  - Generate fingerprint with fingerprintJS
  - 2 sites, embedding each other
  - Test without and with FP-Block

- Run validation
  - BC, IO, TM, fingerprintJS, Panopticlick, AddThis

- Actual test: BlueCava ID request

Monitoring evolution of fingerprinters

Sep 2014 – Sep 2015:

- Panopticlick –
- **BlueCava** *** (2 updates)**
- **AddThis** *** (many updates)**
- **Iovation** **35.7kb, 36.8kb, 35.7kb, 36.8kb, 36.7kb, 37.1kb**
- FingerPrintJS added screen orientation, *****
- **ThreatMetrix** **major changes since 27 oct '14**

Conclusions

- Ubiquitous tracking is a reality
- Countermeasures fall short
- Local tracking is acceptable

Results:

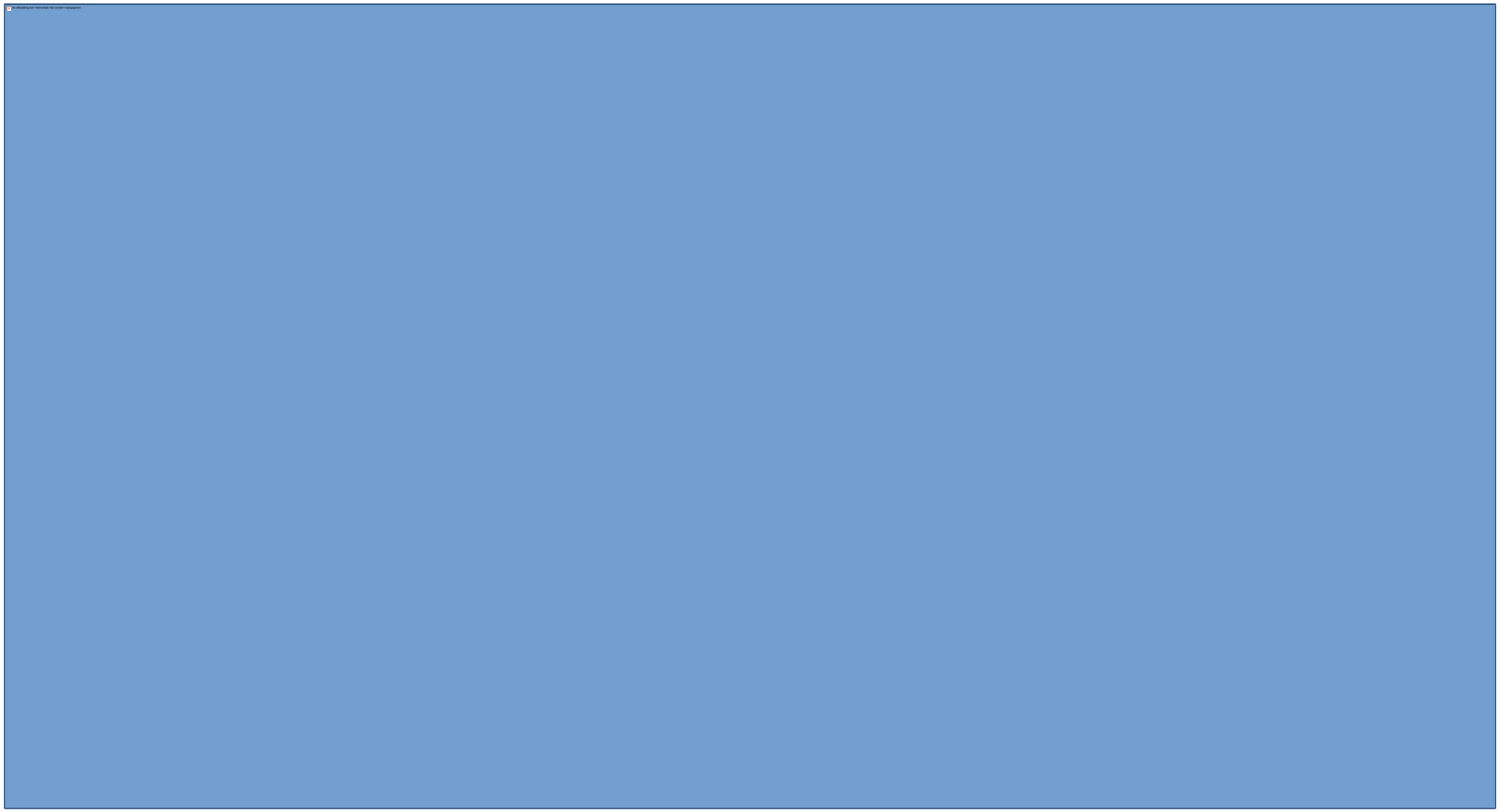
- Propose separation of web identities
- Determine fingerprint vectors
- Proof-of-concept implementation
- Validation against commercial fingerprinters

Current / future work (interested?)

- Boris Arkenaar (Msc):
  webscraping + fingerprinting
- Gabry Vlot (Msc):
  “every webscraper is equal… but are some more equal than others?”
- Benni Krumnow (PhD): **Tracking online data**
- Marc Sleegers (BSc): **Firesheep 7 years later**
- Lucas Vos, Bas Doorn (BSc): **Private Tweeeting**
- Clayton Drazner, Nikola Đuza: **Block Assessor**
- Interested? Hugo.jonker@ou.nl
  Www.open.ou.nl/hjo/supervision.htm

Thank you for your attention!

References (1)



References (2)