Mitigating Browser Fingerprint Tracking: Multi-level Reconfiguration and Diversification

Pierre Laperdrix, Walter Rudametkin, Benoit Baudry

Seams – May, 19th 2015

DiverSE

Diversity-Centric Software Engineering

SEAMS 2015 May 18-19 Firenze, Italy

Inria INVENTEURS DU MONDE NUMÉRIQUE | UNIVERSITÉ DE RENNES 1 | INSA RENNES | cnrs

Table of contents

Tracking users

Cookies

- Installation of a file on the user's computer
- Possibility for the user to delete first and third-party cookies
- Browser extensions can manage and block cookies

Tracking users

Device fingerprinting

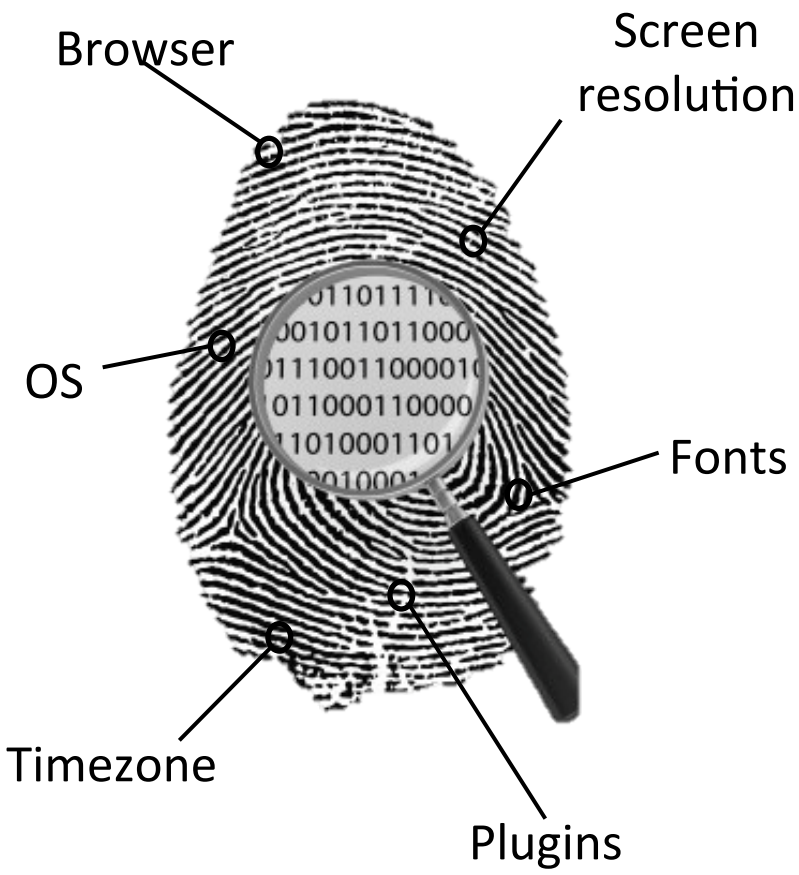
- Side-effect of software diversity
- Collection of information on the device
  - ✓ Browser
  - ✓ Operating system
  - ✓ Hardware


01100110
HTML
Firefox OS

Example of a fingerprint

Attribute	Value
User agent	Mozilla/5.0 (X11; Linux i686; rv:25.0) Gecko/20100101 Firefox/ 25.0
HTTP accept	text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8 gzip, deflate en-US,en;q=0.5
Plugins	Plugin 0: QuickTime Plug-in 7.6.6; libtotem-narrowspace-plugin.so; Plugin 1: Shockwave Flash; Shockwave Flash 11.2 r202; libflashplayer.so;
Fonts	Century Schoolbook, Source Sans Pro Light, DejaVu Sans Mono, Bitstream Vera Serif, URW Palladio L, Bitstream Vera Sans Mono, Bitstream Vera Sans, ...
HTTP DoNotTrack	1
Cookies enabled	Yes
Platform	Linux i686
OS	Linux 3.14.3-200.fc20.x86 32-bit
Screen resolution	1920x1080x24
Timezone	-480
DOM Session storage	Yes
DOM Local storage	Yes
I.E. User data	No

How unique and trackable are we?



Panopticlick
How Unique – and Trackable – Is Your Browser?

- 83.6% of unique fingerprints

Am I Unique?

- 86.4% of unique fingerprints

How widespread is fingerprinting?

Google

- **Device information**

We may collect **device-specific information** (such as your hardware model, operating system version, unique device identifiers and mobile network information including phone number). Google may associate your **device identifiers** or **phone number** with your Google Account.

Yahoo

Yahoo automatically receives and records information from your computer and browser, including your IP address, Yahoo cookie information, software and hardware attributes, and the page you request.

Amazon

Automatic Information

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information

Twitter

Log Data: Our servers automatically record information ("**Log Data**") created by your use of the Services. Log Data may include information such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites,

Device fingerprinting

- Silent
- Complement usage of cookies
- Hard to detect and block fingerprinting scripts
- Already adopted by major web actors
- Track users without their knowledge
- Real privacy problem

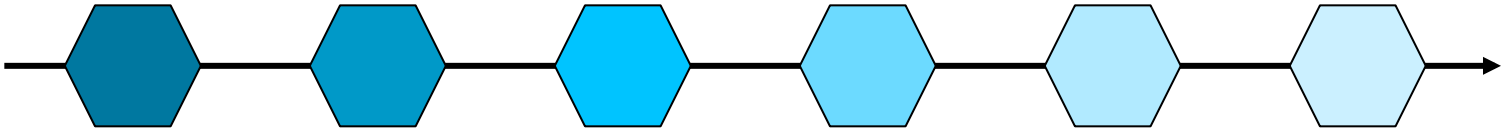
Table of contents

Properties of a fingerprint

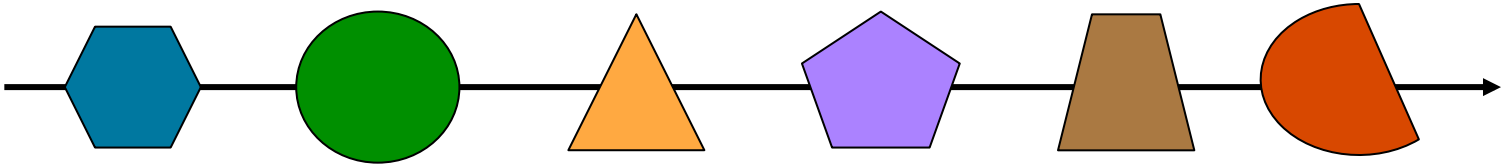
- Uniqueness: we can precisely identify a device thanks to its unique combination of features
- Stability: a fingerprint does not drastically change over time
- These two properties combined are the source of a real privacy problem.

Blink

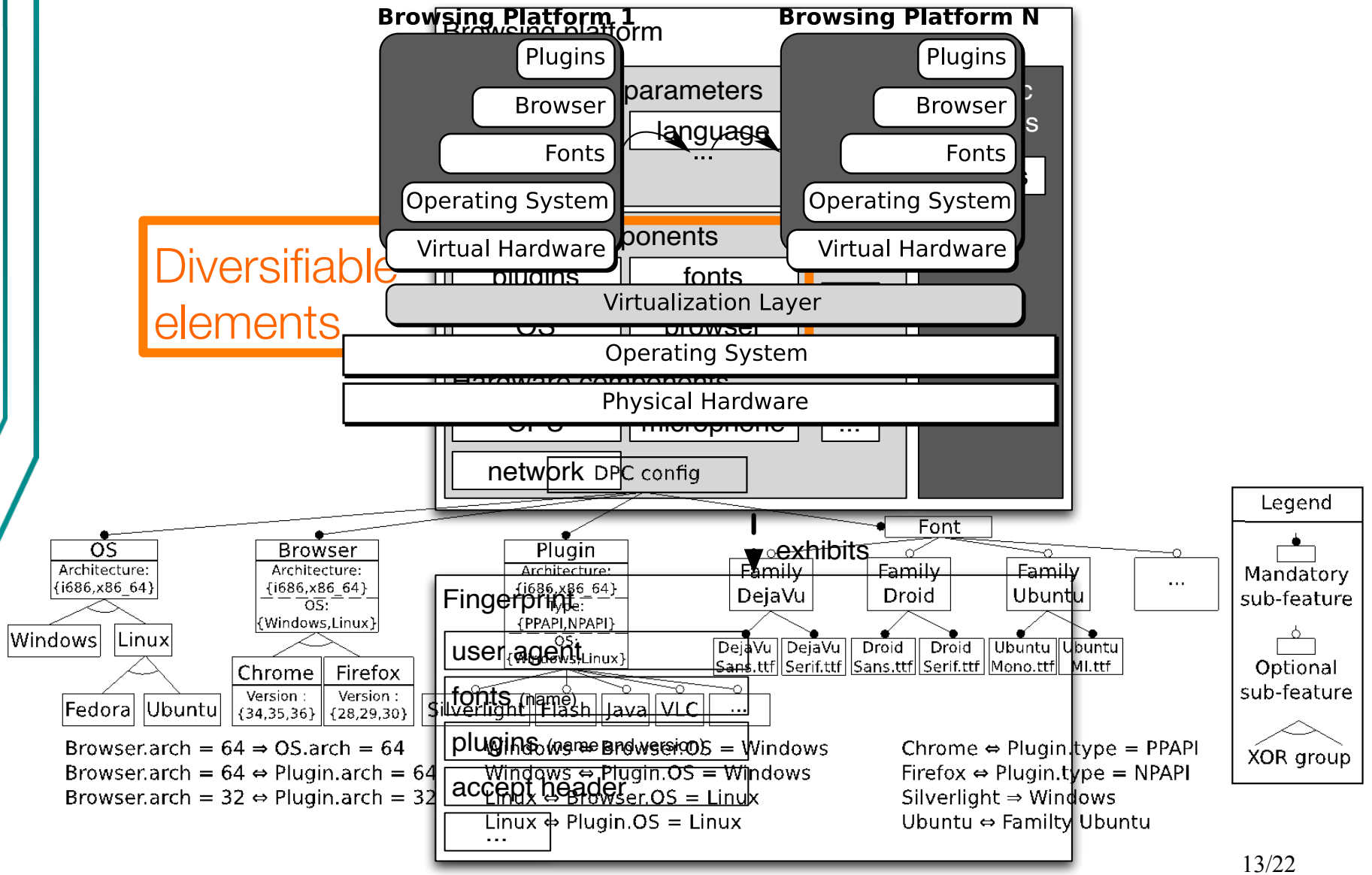
- Increase temporal diversity of fingerprints.
- Reconfigure platform at runtime.
- No lies.
- Browsing without Blink



- Browsing with Blink



Browsing platform



Blink's generation process

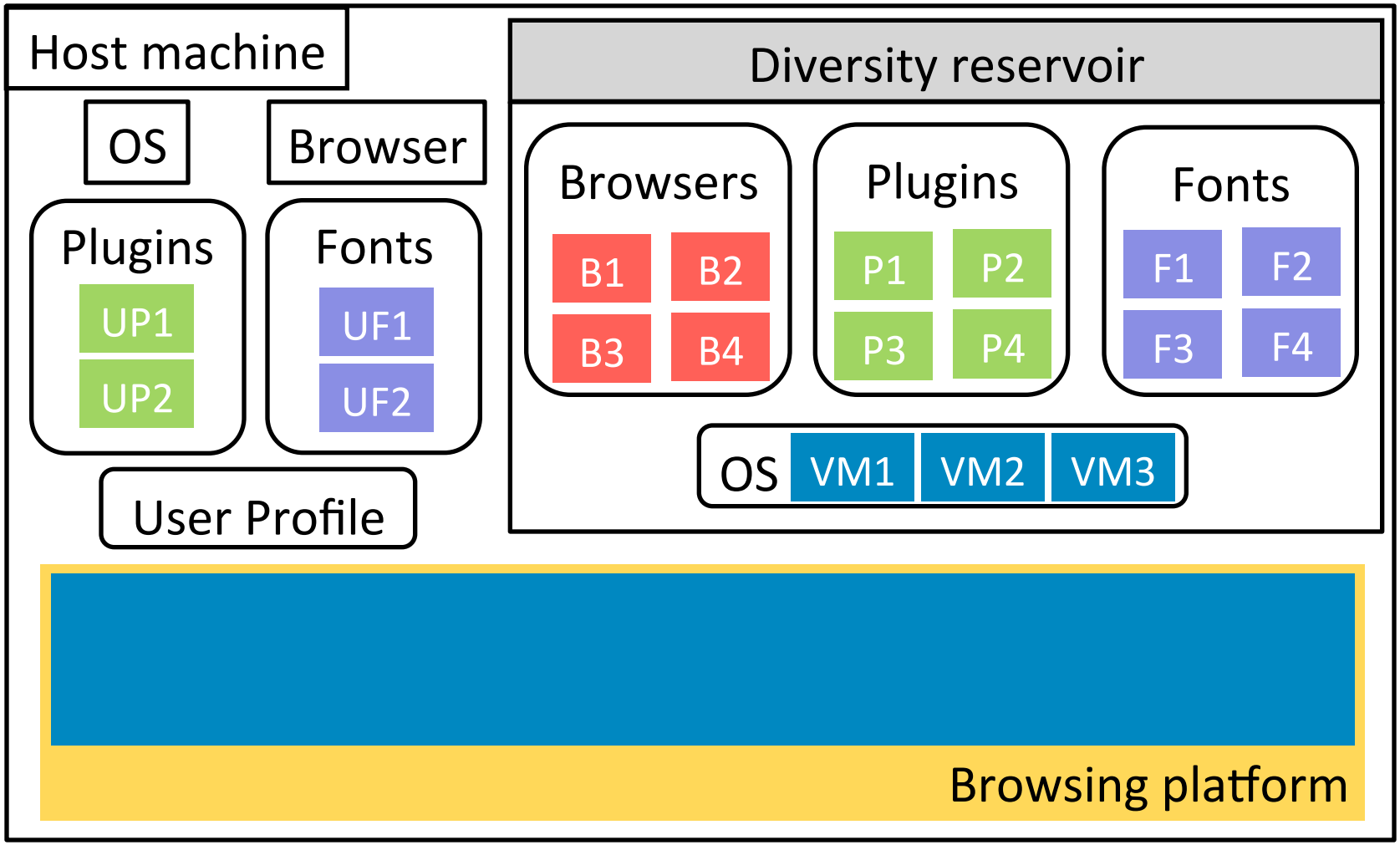


Table of contents

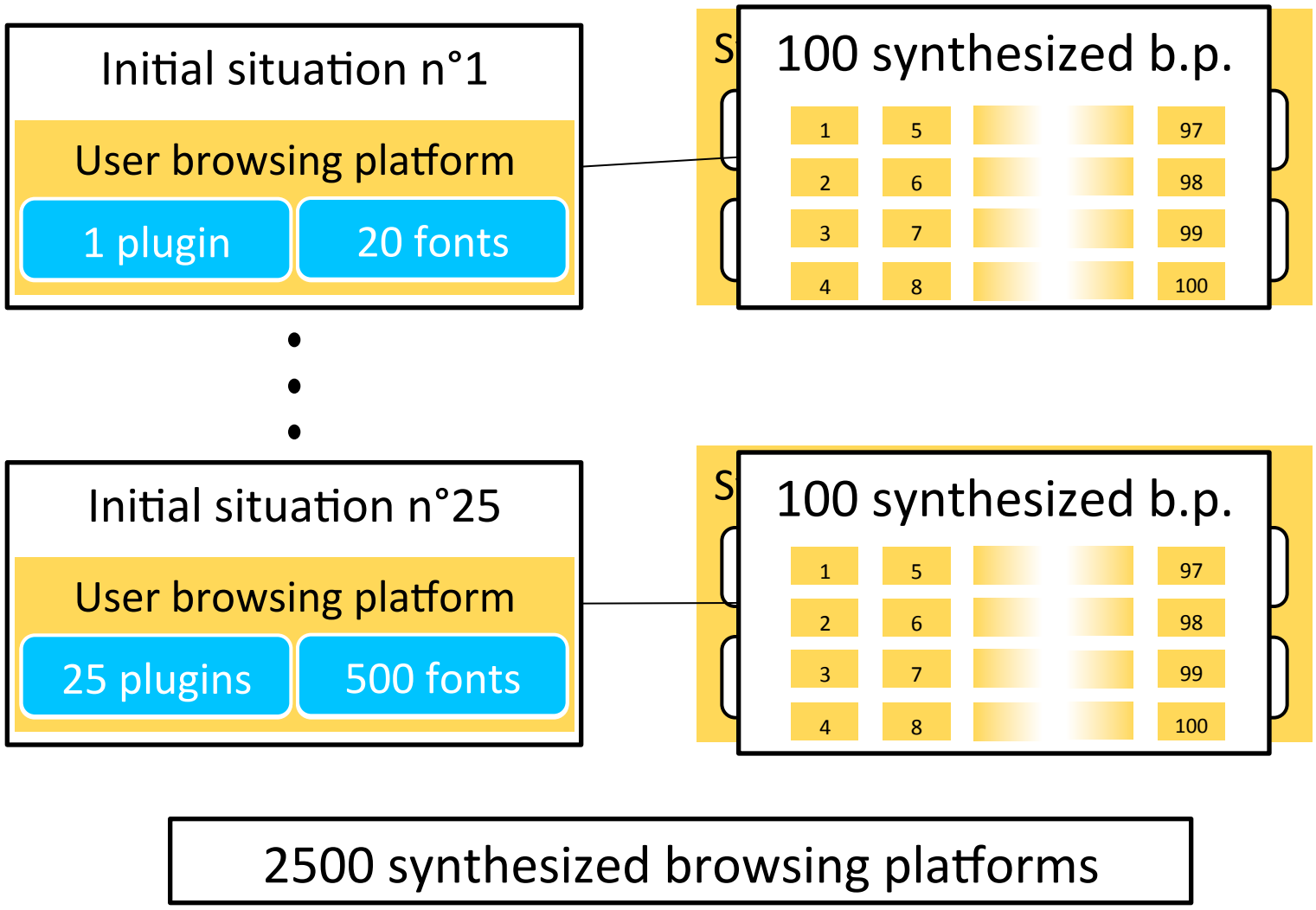
Objectives

1. Does dynamic reconfiguration break fingerprint stability?
2. What is the impact of the user's plugins and fonts on global diversity?

Requirements

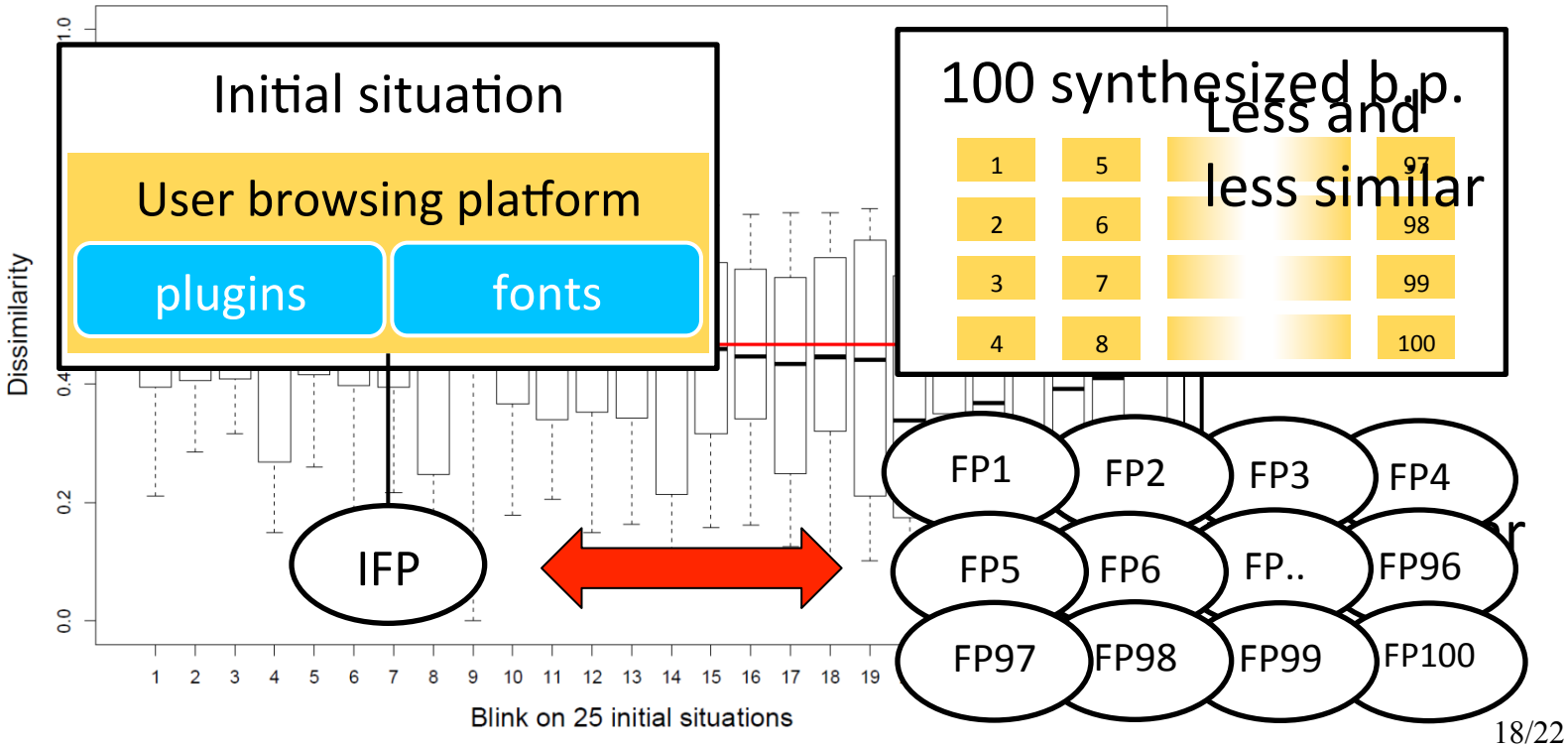
- A fingerprinting script
- A metric to quantify the difference between two synthesized platforms

Experimental protocol



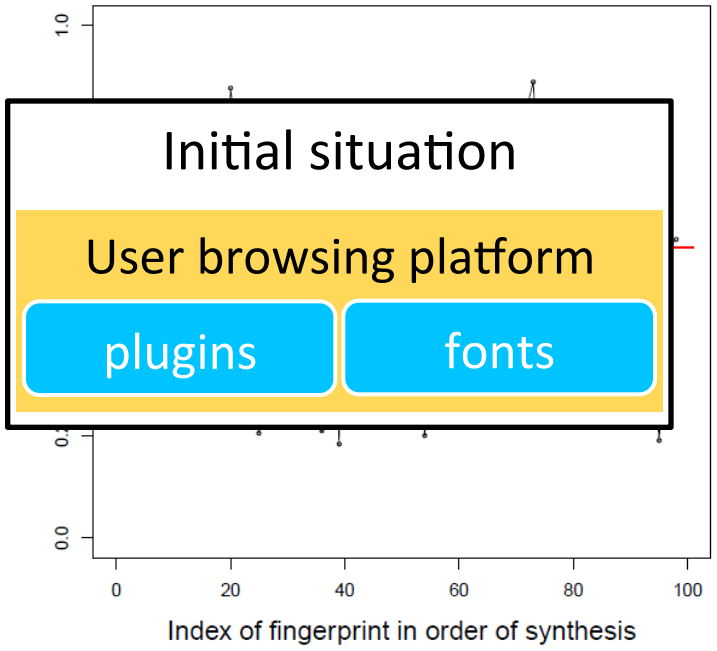
Research questions

1. How different from the original user's fingerprint are the fingerprints exhibited by the synthesized platform?



Research questions

2. How diverse is the set of fingerprints exhibited by the synthesized platforms?



(a) 1 plugin in initial environment

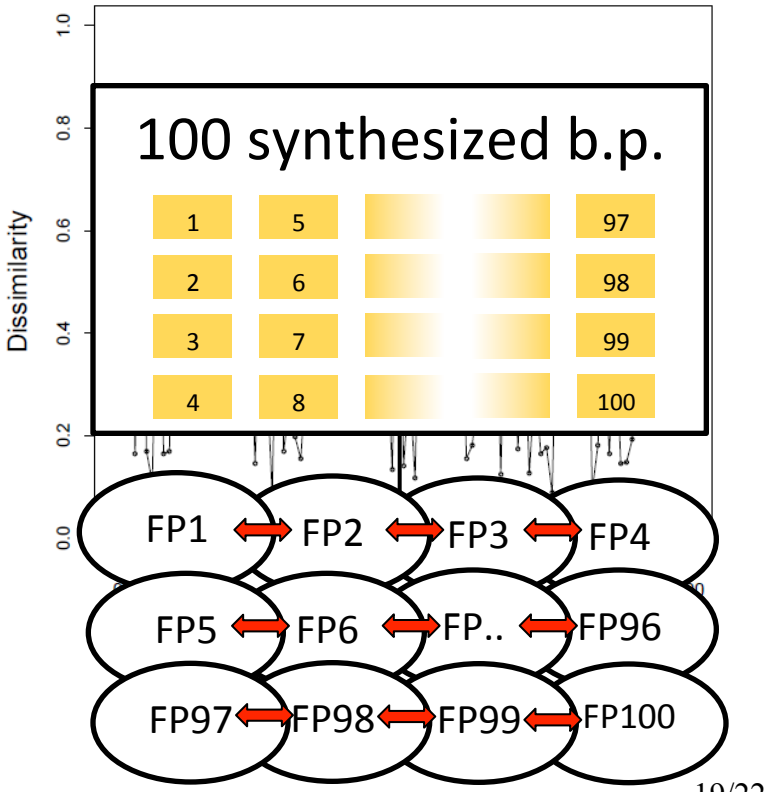


Table of contents

Conclusion and perspectives

- Blink: break fingerprint stability thanks to automatic and complete synthesis of a new browsing platform for each browsing session
- AmIUnique.org: Collection of fingerprints to refine Blink's randomization algorithms https://amiunique.org
- Blink on Docker: Fast and lightweight prototype already available https://github.com/plaperdr/blink-docker

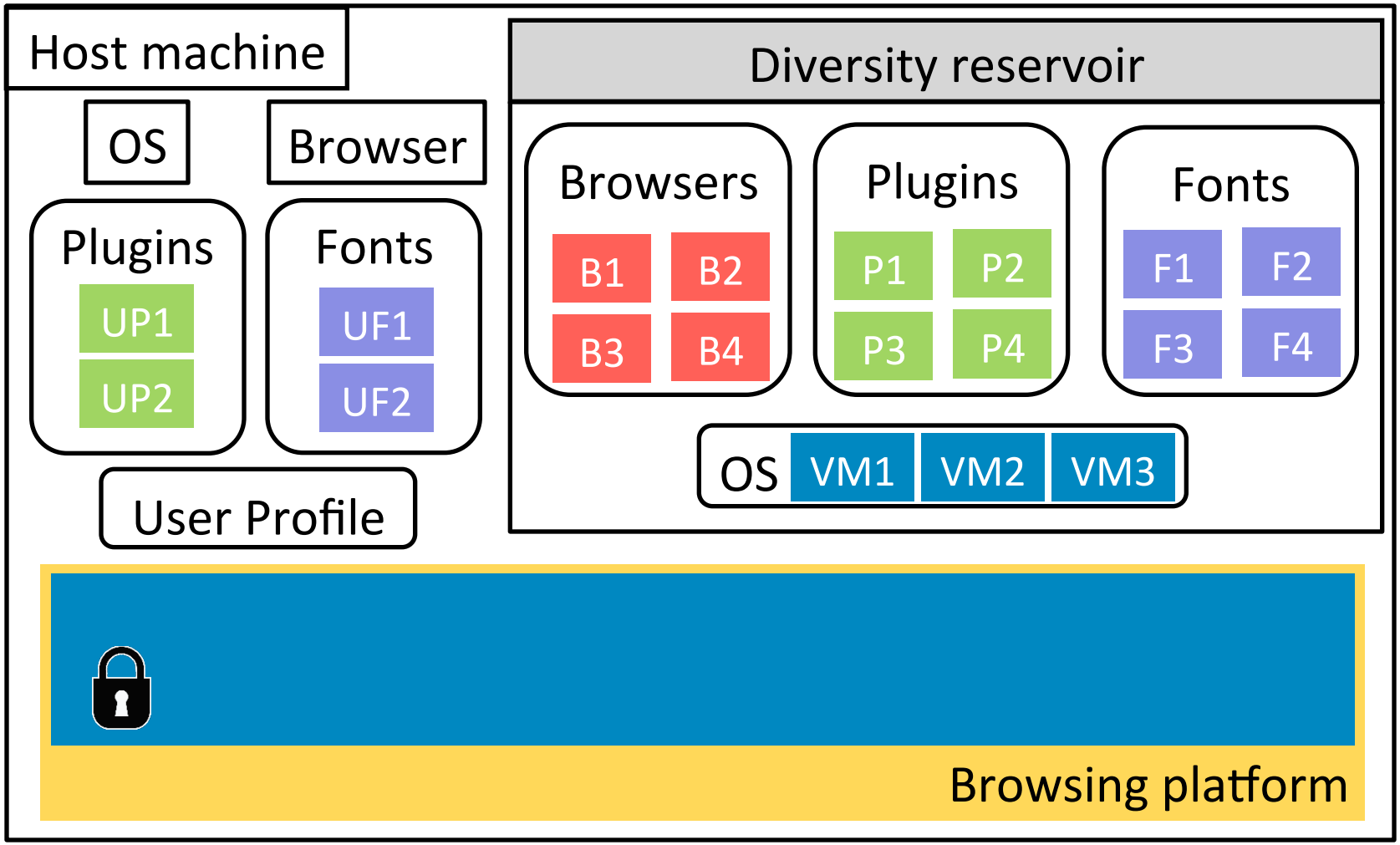
Thank you for listening!

Any questions?

Summary of current solutions

Solution	Focus	Comments
Blocking extension	Blocking	Does not block everything
Spoofing extension	Lying	Creates detectable inconsistencies
Multiple browsers	Increasing diversity	Decreases usability and is inefficient
Tor browser	Removing diversity	Decreases usability
Blink	Increasing diversity and changing fingerprint for each browsing session	No inconsistencies, no decrease in usability, no brittleness

Blink's Coffee break mode



Comparison with cookies