06. Protection from Browser fingerprinting

Nataliia Bielova

@nataliabielova

September 17th=21st, 2018

Web Privacy course

University of Trento

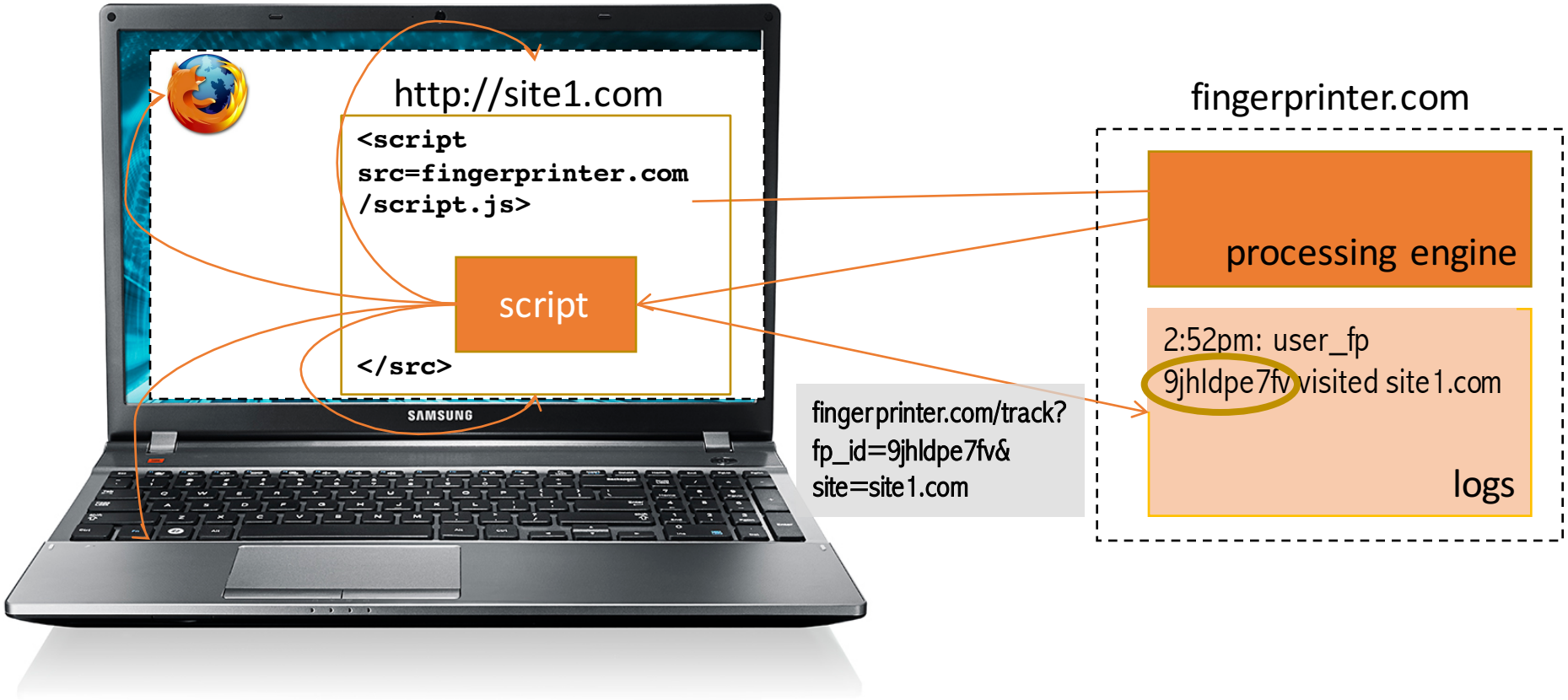
Example of a browser fingerprint

Attribute	Value
User agent	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
HTTP headers	text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8 gzip, deflate, br 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 26.0 r0; 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, ...
Platform	Linux x86_64
Screen resolution	1920x1080x24
Timezone	-480 (UTC+8)
OS	Linux 3.14.3-200.fc20.x86 32-bit
WebGL vendor	NVIDIA Corporation
WebGL renderer	GeForce GTX 650 Ti/PCIe/SSE2
Canvas	Cwm fjordbank glyphs vext quiz, 😀 Cwm fjordbank glyphs vext quiz, 😀

Slides courtesy of Pierre Laperdrix (Stony Brook University)

Browser fingerprinting used for tracking

Browser and operating system properties are used to track repeated visits to a site.



Outline

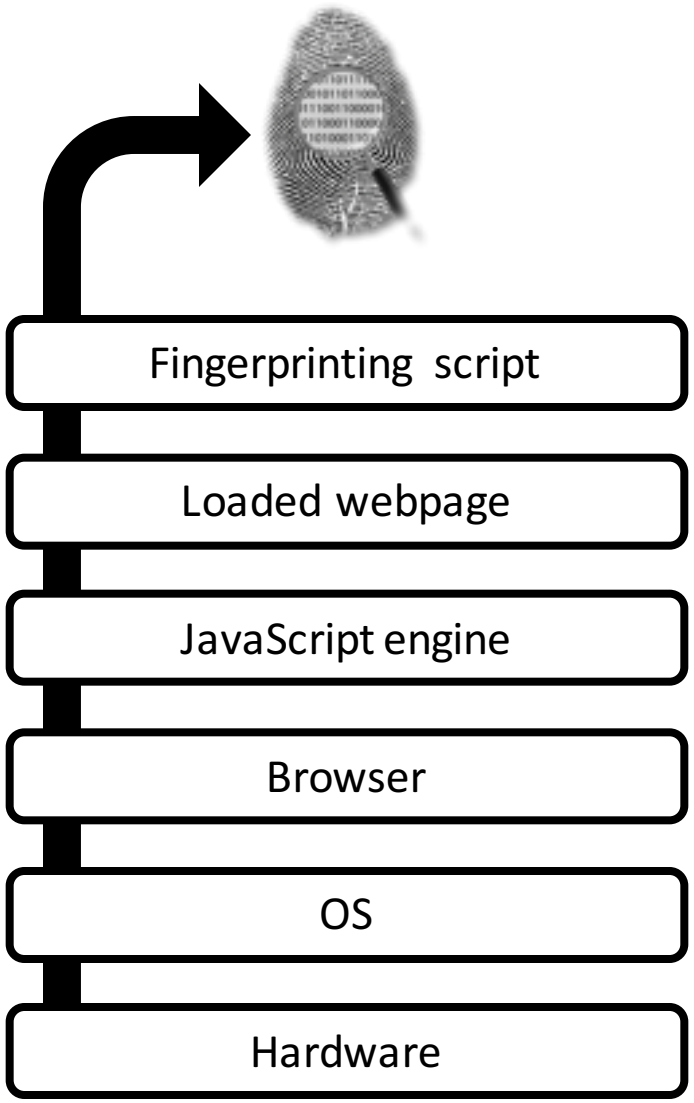
I. What is browser fingerprinting?

II. Defenses against browser fingerprinting

Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Defending against fingerprinting

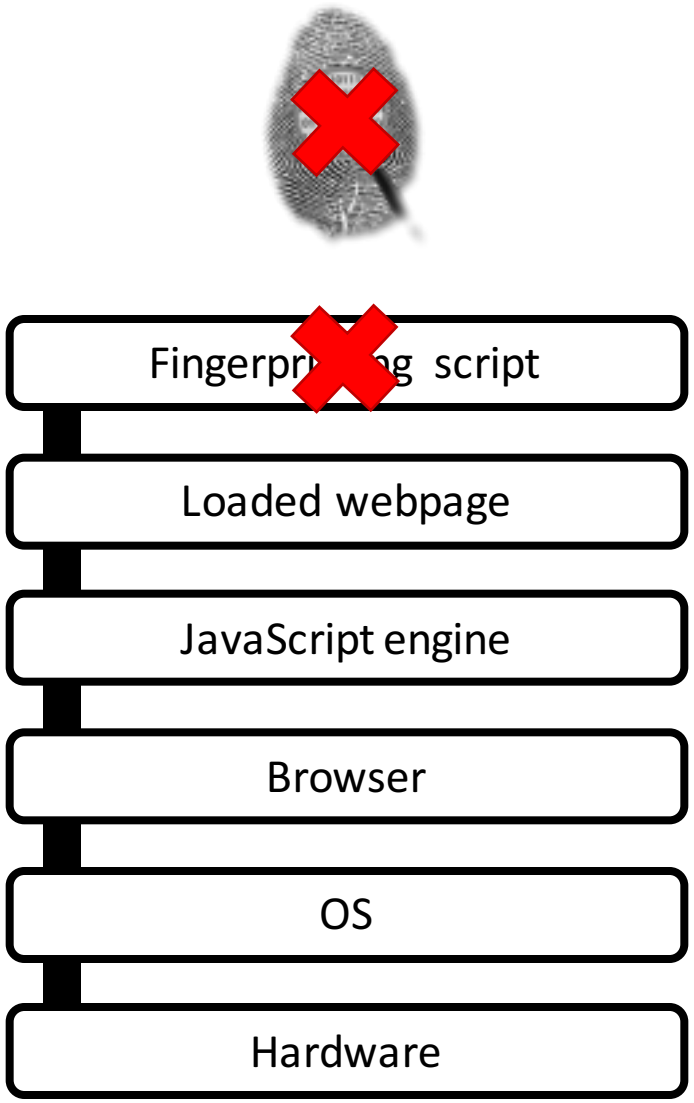
- Goal: to protect users against browser fingerprinting, i.e. to prevent them from being tracked online



Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Blocking scripts

- The fingerprinting script is simply not executed.



II. Blocking scripts

- Browser extensions or built-in in the browser

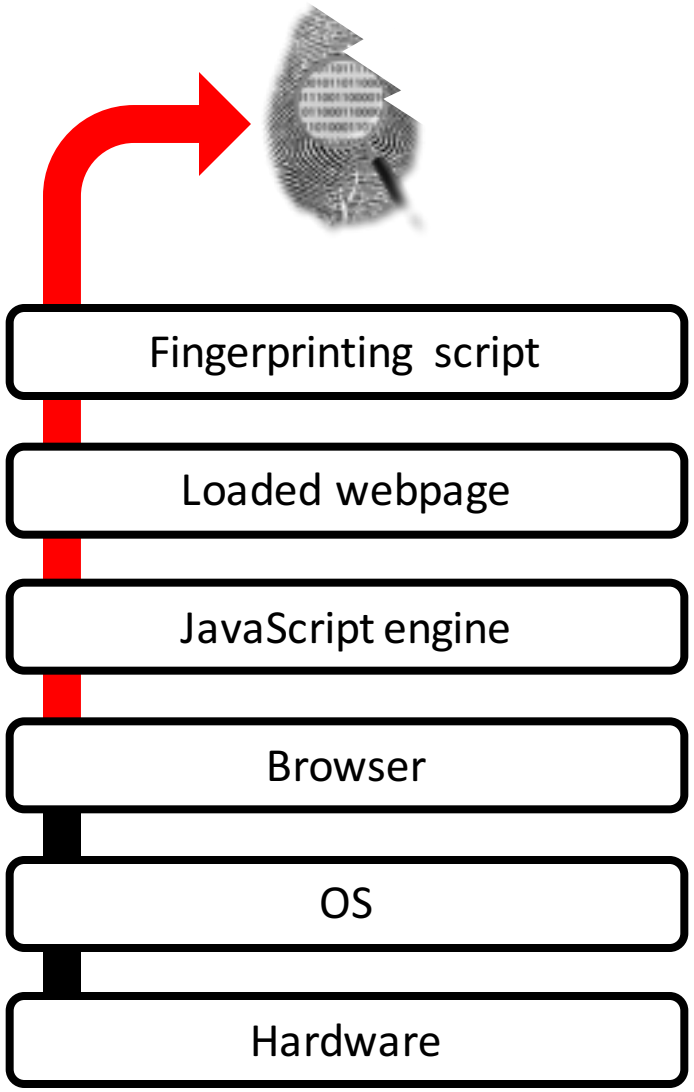
uBlock | Ghostery | Disconnect | Brave | Firefox (by default in private mode)

- Pros: Easy to install and to use. Transparent to the user.
- Cons: This technique revolves around up-to-date blacklists. User is vulnerable if the fingerprinting script is not in the database.

Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Blocking browser APIs

- The fingerprinting script will collect less information.



Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Blocking browser APIs

- Browser extensions or built-in in the browser

CanvasBlocker

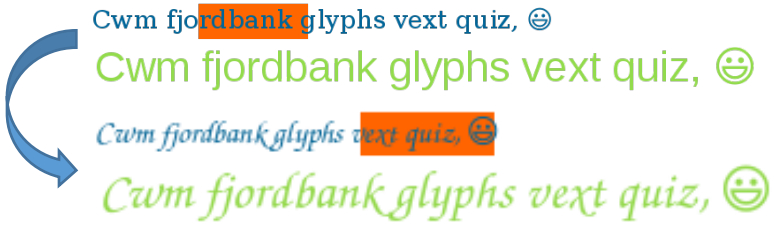
Brave

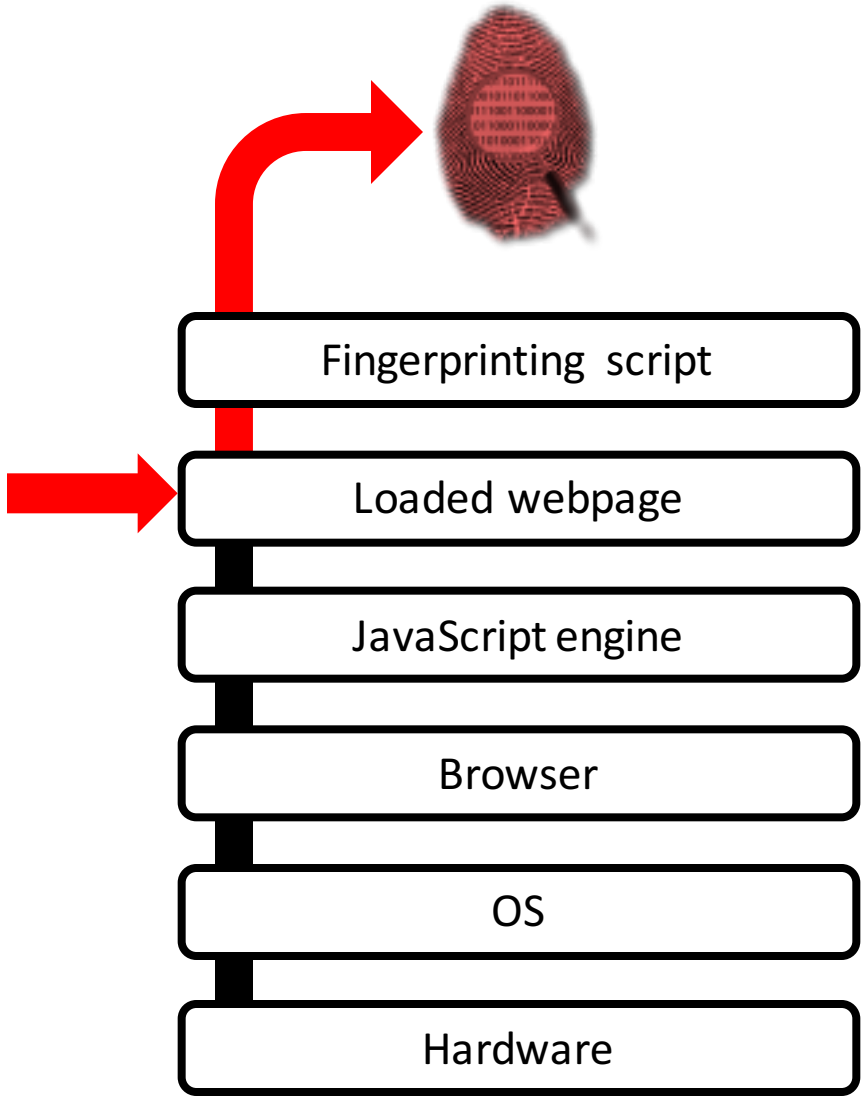
- Pros: Easy to install and to use. Transparent to the user.
- Cons: Only limits the amount of collected information.

Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Injecting JavaScript

- The injection of JavaScript overwrites the default methods of the JavaScript engine.
- Can change values
  - → Default: “Win64”
  - → New value: “Linux x86_64”
- Can inject noise





Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Injecting JavaScript

- Browser extensions

Canvas Defender

Random Agent Spoofer

User-Agent Switcher

- Pros: Easy to install and to use. Transparent to the user.
- Cons: Can easily be detected and creates inconsistencies.

Slides courtesy of Pierre Laperdrix (Stony Brook University)

Mon empreinte

Attribut	Ratio de similarité	Valeur
En-tête "User agent"	<0.1%	"Mozilla/5.0 (compatible; MSIE 10.0; Windows Phone 8.0; Trident/6.0; IEMobile/10.0; ARM; Touch; NOKIA; Lumia 520)"
En-tête "Accept"	59.07%	"text/html,application/xhtml+xml,application/xml;q=0.9;*/*;q=0.8"
En-tête "Content encoding"	63.30%	"gzip, deflate"
En-tête "Content language"	9.64%	"fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3"
Liste des plugins	<0.1%	"Plugin 0: Microsoft Office 2013; The plugin allows you to have a better experience with Microsoft Lync; npMeetingJoinPluginOC.dll. Plugin 1: Microsoft Office 2013; The plugin allows you to have a better experience with Microsoft SharePoint; NPSPWRAP.DLL. "
Plateforme	46.32%	"Win32"
Utilisation des cookies	83.73%	"yes"
Utilisation du Do Not Track	54.33%	"NC"
Fuseau horaire	3.17%	"-120"
Résolution de l'écran	6.96%	"1920x1200x24" → 480 x 800

II. Tor browser and its fingerprint

- In theory, all fingerprints from the Tor Browser should be identical.
- In reality, differences can still be found (screen resolution, platform…).

Tor browser on Fedora 25

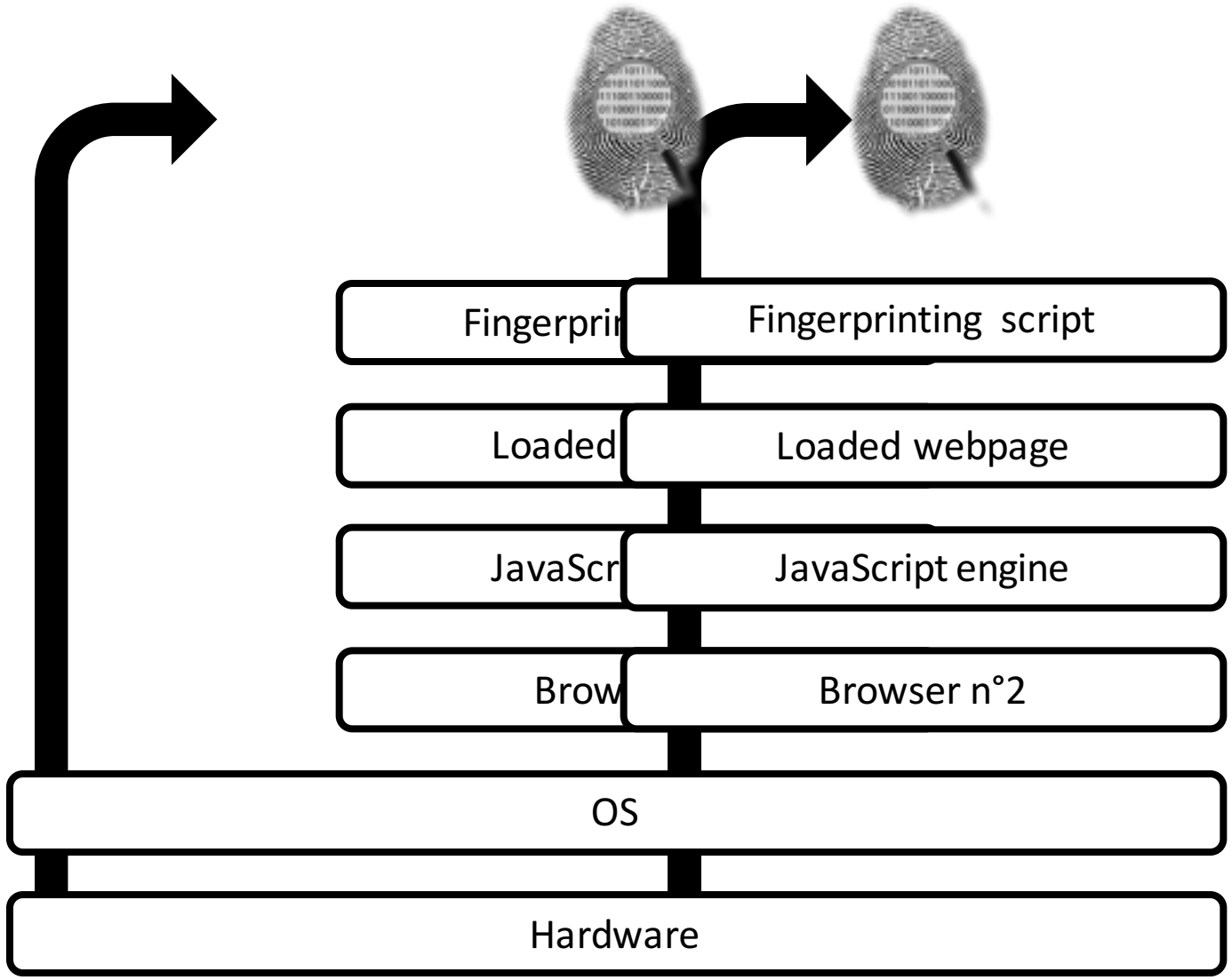
Attribute	Value
User agent	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9;*/*;q=0.8
Content encoding	gzip, deflate, br
Content language	en-US,en;q=0.5
List of plugins	
Platform	Win32
Cookies enabled	yes
Do Not Track	NC
Timezone	0
Screen resolution	1000x1000x24
Use of local storage	yes
Use of session storage	yes
Canvas	
WebGL Vendor	Not supported
WebGL Renderer	Not supported
List of fonts	Flash not detected
Screen resolution	Flash not detected
Language	Flash not detected
Platform	Flash not detected
Use of AdBlock	no

Firefox browser on Fedora 25

Attribute	Value
User agent	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content encoding	gzip, deflate, br
Content language	en-US,en;q=0.5
List of plugins	
Platform	Linux x86_64
Cookies enabled	yes
Do Not Track	yes
Timezone	-120
Screen resolution	1920x1200x24
Use of local storage	yes
Use of session storage	yes
Canvas	Cwm fjordbank glyphs vext quiz, 😀 Cwm fjordbank glyphs vext quiz, 😀
WebGL Vendor	Intel Open Source Technology Center
WebGL Renderer	Mesa DRI Intel(R) Haswell Mobile
List of fonts	Flash not detected
Screen resolution	Flash not detected
Language	Flash not detected

II. Changing browsers

- One fingerprint for each browser
- One profile for each fingerprint
- The OS and Hardware layers are shared by both fingerprints.



Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Changing browsers

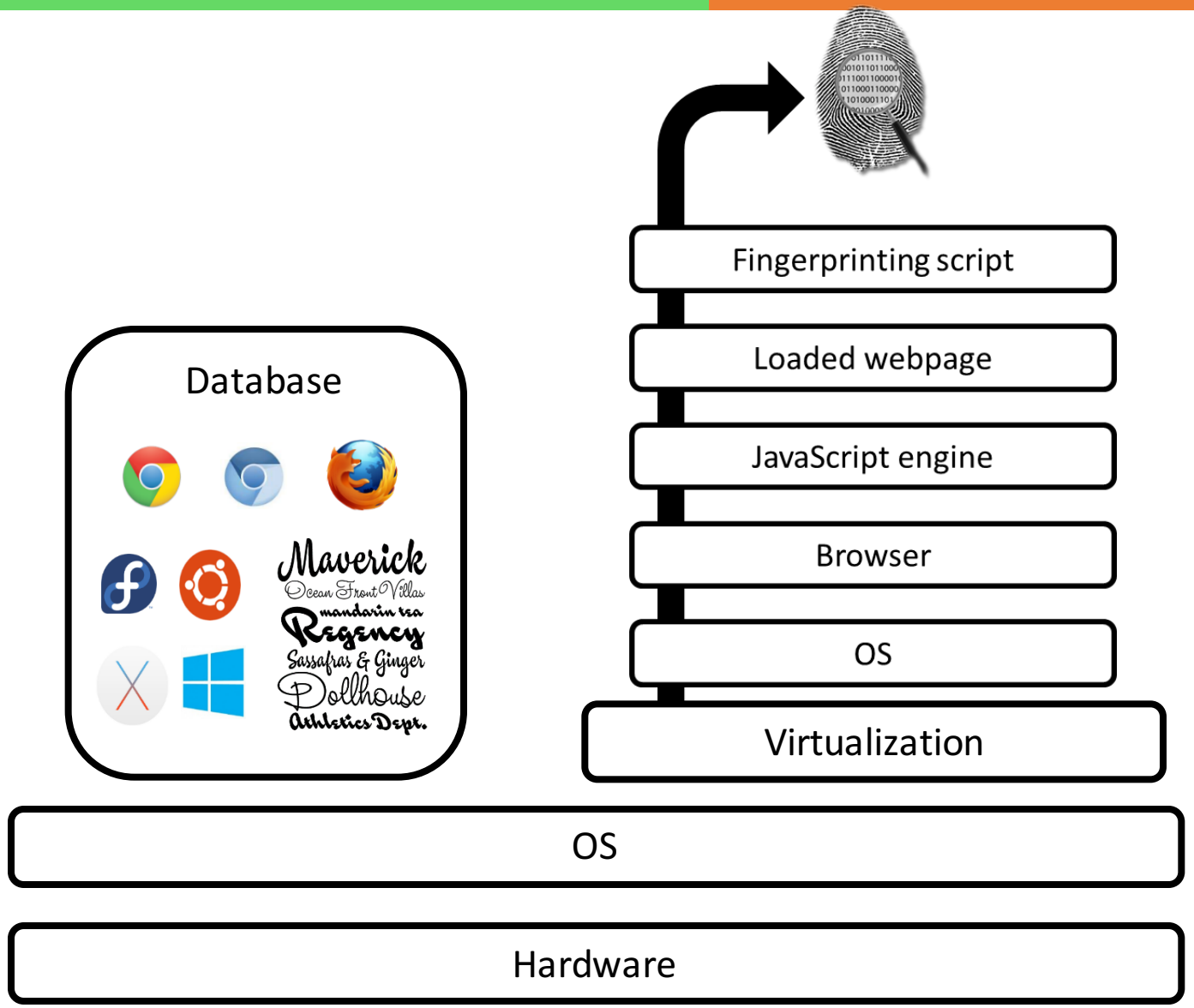
- Browsers

- Pros: Anybody can switch between any browsers.
- Cons: Cross-browser fingerprinting exists. By collecting enough information on the OS and hardware, one can still be identified.

➢See uniquemachine.org (WebGL tests)

II. Recreating a complete environment

- Disposable environments with a unique fingerprint for each browsing session
- Database with different OS, fonts, plugins and browsers
- Use of virtualization to isolate the host OS from the new environment

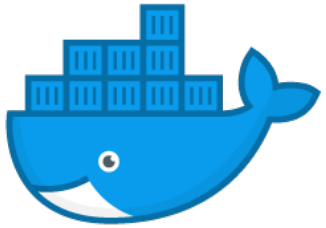


Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Recreating a complete environment

- Academic prototype called Blink

Version on VirtualBox
https://github.com/DIVERSIFY-project/blink



Version on Docker
https://github.com/plaperdr/blink-docker

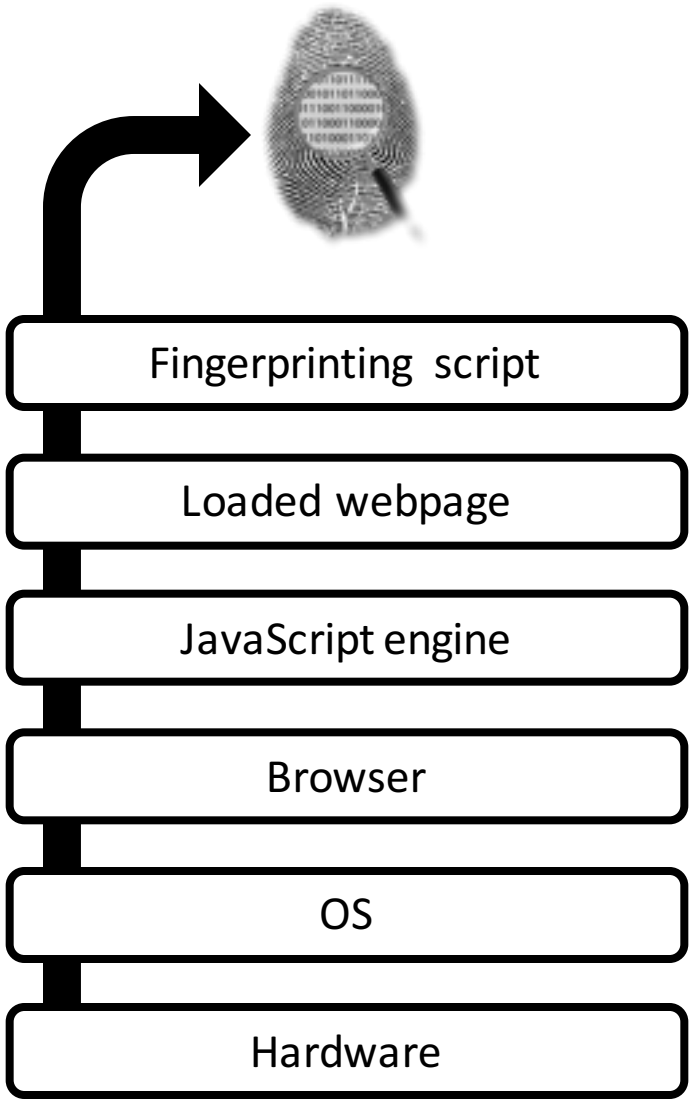
- Pros: Does not create inconsistencies in fingerprint. The components truly exist.
- Cons:
  - High resources consumption (disk space, CPU).
  - The usability is not as good as other solutions.

Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Summary of defense techniques

Many different approaches:

- Blocking scripts
- Blocking browser APIs
- Injecting JavaScript
- Native spoofing
- Changing browsers
- Recreating complete environments



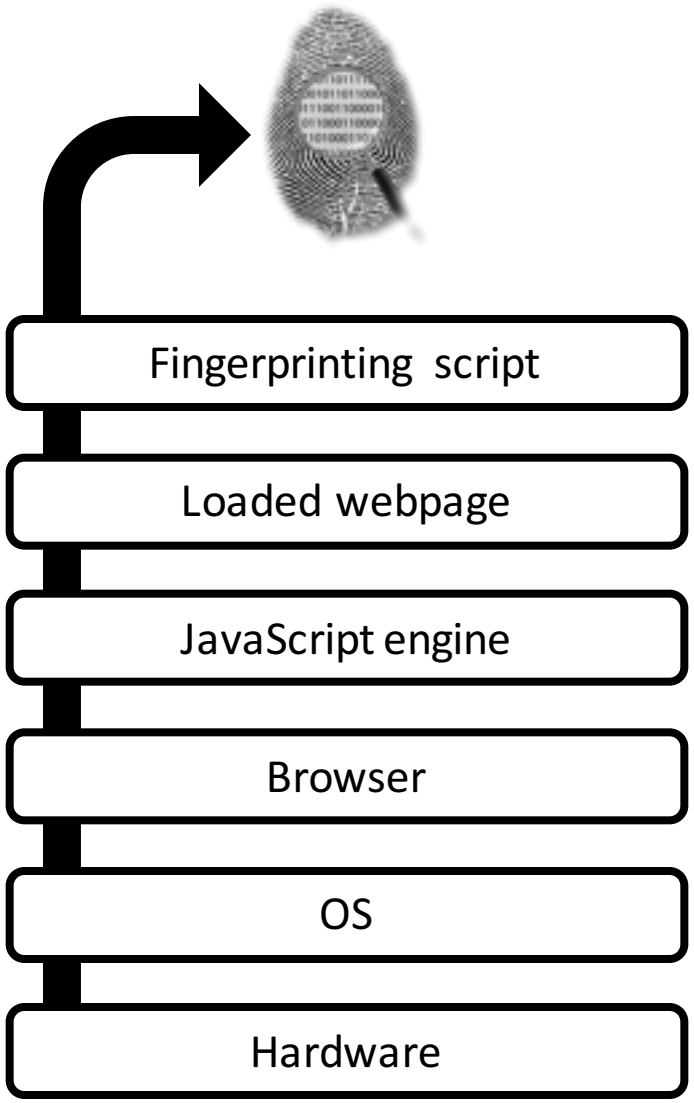
Slides courtesy of Pierre Laperdrix (Stony Brook University)

II. Summary of defense techniques

No ultimate solutions

- Each one has its pros and cons.
- It is always a complicated tradeoff between protection and usability.

Easiest solution to put in place: block fingerprinting scripts.



Slides courtesy of Pierre Laperdrix (Stony Brook University)

Conclusion

- **Browser fingerprinting** is a stateless tracking technique that relies on the collection of information about a user's device and its configuration.
- This technique is a **side-effect** of the way the web and browsers have been built for the past two decades. A single patch cannot fix the problem.
- Protecting users against fingerprinting is complicated. **Many different approaches** are possible with each their pros and cons.

Slides courtesy of Pierre Laperdrix (Stony Brook University)