Browser Extension and Login-Leak Experiment

http://extensions.inria.fr

Gábor Gulyás, Nataliia Bielova, and Claude Castelluccia

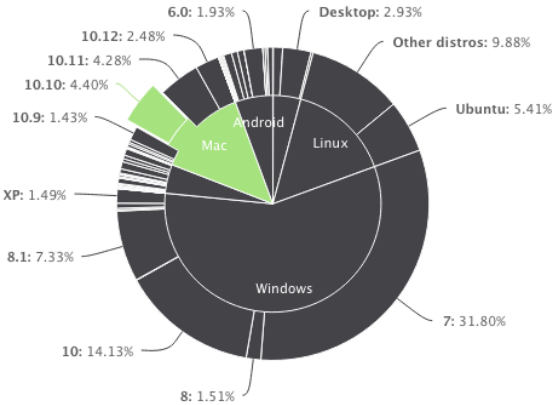
Device fingerprinting

https://amiunique.org

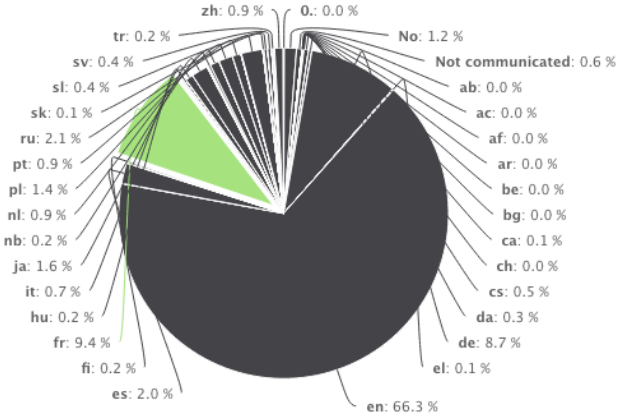
My fingerprint

Attribute	Similarity ratio	Value
User agent	<0.1%	"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:53.0) Gecko/20100101 Firefox/53.0"
Accept	57.16%	"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
Content encoding	22.79%	"gzip, deflate, br"
Content language	<0.1%	"fr-FR,en-US;q=0.7,en;q=0.3"
List of plugins	<0.1%	"Plugin 0: Shockwave Flash; Shockwave Flash 25.0 r0; Flash Player .plugin. "
Detail of the plugins		
	47.53 %	Shockwave Flash
Platform	11.94%	"MacIntel"
Cookies enabled	77.49%	"yes"

Operating systems



Languages



Behavioral fingerprinting

http://extensions.inria.fr

DEMO

- Browser extension detection
- ~13 000 extensions

- Websites a user is logged in
- 58 websites

Browser extension detection

- via **Web Accessible Resources**

chrome-extension://gpdjojdkbbmdfjfahjcgigfpmkopogic/img/icon_48.png

unique extension ID

Discovering Browser Extensions via Web Accessible Resources

Alexander Sjösten
Chalmers University of Technology
Gothenburg, Sweden
sjosten@chalmers.se

Steven Van Acker
Chalmers University of Technology
Gothenburg, Sweden
acker@chalmers.se

Andrei Sabelfeld
Chalmers University of Technology
Gothenburg, Sweden
andrei@chalmers.se

ABSTRACT

Browser extensions provide a powerful platform to enrich browsing experience. At the same time, they raise important security questions. From the point of view of a website, some browser extensions are invasive, removing intended features and adding unintended ones, e.g. extensions that hijack Facebook likes. Conversely, from the point of view of extensions, some websites are invasive, e.g. websites that bypass ad blockers. Motivated by security goals at clash, this

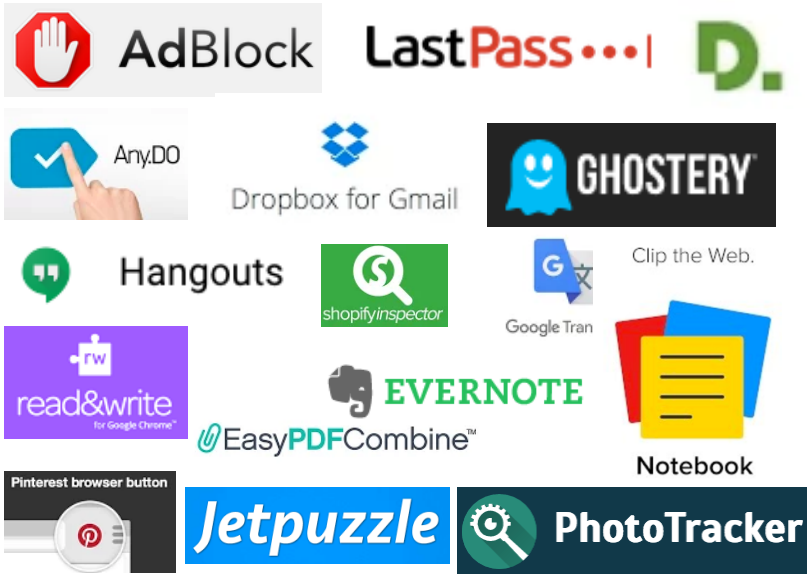
The first and second scenarios present an exclusive point of view of websites, concerned with malicious extensions. The third scenario presents an exclusive view of extensions, concerned with malicious websites. The fourth scenario illustrates legitimate synergies between websites and extensions. Finally, the fifth scenario illustrates the security goals of websites and extensions at outright clash.

Bank scenario Bank webpages manipulate sensitive information whose unauthorized access may lead to financial

Behavioral fingerprinting

http://extensions.inria.fr

- Browser extension detection
- ~13 000 extensions



- Websites a user is logged in
- 58 websites

Detection of websites a user logged in

- Redirection URL hijacking [@robin_linus]

Your Social Media Fingerprint

Without your consent most major web platforms leak whether you are logged in. This allows any website to detect on which platforms you're signed up. Since there are lots of platforms with specific demographics an attacker could reason about your personality, too.

This project is an open source contribution of **RobinLinus** - Security, Privacy & Blockchain Consulting.

Demonstration

You are logged in to:

Twitter

- Abusing Content Security Policy (CSP) – no JavaScript needed [@homakov]

Monday, January 13, 2014

Using Content-Security-Policy for Evil

TL;DR How can we use technique created to protect websites for Evil? (We used XSS Auditor for Evil before) There's a neat way: taking advantage of CSP we can detect whether URL1 does redirect to URL2 and even bruteforce /path of URL2/path. This is a conceptual vulnerability in CSP design (violation == detection), and there's no obvious way to fix it.

Demo & playground: http://homakov.github.io/csp.html

Redirection URL hijacking

redirection URL

https://cas.inria.fr/cas/login?service=
https%3A%2F%2Fwww.inria.fr%2Fextension%2Fsite_inria
%2Fdesign%2Fsite_inria%2Fimages%2Flogos
%2Flogo_INRIA.png

resource available to logged in users only

Not logged in
(login page)

Logged in
(silent & unchecked
redirection to image)

Abusing Content Security Policy

(CSP allows resources only from this URL)

https://fr.linkedin.com

Not logged in
Login page appears
at fr.linkedin.com

Logged in
Redirects to
www.linkedin.com

But: also reports a CSP violation!

Main page News & Updates How it works F.A.Q. Privacy policy

Browser Extension and Login-Leak Experiment

When you browse the web, small beacons (trackers) are spying on your online activities. Even though such trackers are invisible, they collect information about you such as which pages you visit, which buttons clicked, and what text you typed. This information is often used to show you targeted advertisements and may require you to pay a higher price during online shopping depending on the collected information.

Did you know websites can track you by your browser extensions and web logins?

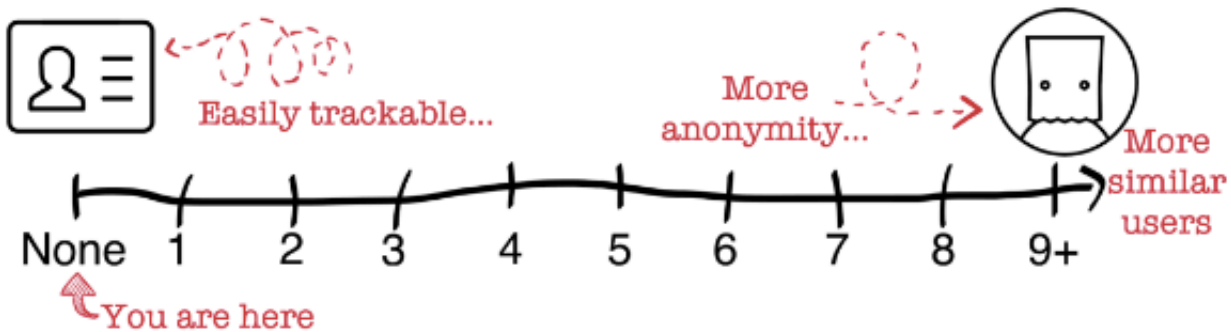
Recent studies show that you can be tracked based on your web browser properties. In this experiment, we demonstrate that you can also be tracked by

- your browser extensions (such as AdBlock, Pinterest, or Ghostery), and
- the websites you have logged in (such as Facebook, Gmail, or Twitter).

You can learn more here about how these detection techniques work.

Are you identifiable?

Yes, you are identifiable, as there are no other users who looks like you among the 17275 users we tested so far:



Are you identifiable...

...by your extensions?	yes
...by your website logins?	no
...by your browser fingerprint?	no
...by your extensions, web logins and browser fingerprint together?	yes

Standard fingerprint details

Your browser's standard fingerprint **is not unique**! We found 1578 collision(s) among the 17298 browsers tested so far!

Detected browser properties:

User agent:	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Resolution (available):	1280x800 (1280x773)
Timezone:	-120
Language:	en-US
Detected fonts: (ca. 500 fonts tested in JavaScript)	MT Script Capitals, Meiryo, Microsoft Himalaya, Microsoft Tai Le, Microsoft Yi Baiti, MingLiU, MingLiU_HKSCS, MingLiU_HKSCS-ExtB, MingLiU-ExtB, Mistral, Modern No. 20, Mongolian Baiti, MS Mincho, MS PMincho, MS Reference Specialty, MT Extra, Nadeem, Noteworthy, Onyx, OPTIMA, Oriya Sangam MN, OSAKA, Papyrus, Perpetua, Perpetua Titling MT, Plantagenet Cherokee, Playbill, PMingLiU, PMingLiU-ExtB, Rockwell, Rockwell Extra Bold, Savoye LET, SimHei, SimSun, SimSun-ExtB, Sinhala Sangam MN, Skia, Snell Roundhand, Stencil, Tamil Sangam MN, Telugu Sangam MN, Thonburi, Tw Cen MT, Vivaldi, Wide Latin, Zapfino
List of plugins	Widevine Content Decryption Module::Enables Widevine licenses for playback of HTML audio/video content. (version: 1.4.8.970)::application/x-ppapi-widevine-cdm~Shockwave Flash::Shockwave Flash 25.0 r0::application/x-shockwave-flash~swf,application/futuresplash~splChrome PDF Viewer::::application/pdf~pdfNative

Browser extension details

Your browser's extension fingerprint is **unique** among the 17275 browsers tested so far!

Tested extensions:

13462/13462

adblock	chrome-extension://gighmmpiobklfepjocnamgkkbiglidom/adblock-jquery-ui.custom.css
ghostery	chrome-extension://mlomiejdfkolichcflejclcbmpeaniij/app/images/apps_pages/tracker.pn
pinterest-save-button	chrome-extension://gpdjojdkbbmdfjfahjcgigfpmkopogic/img/icon_48.png

Website login details (login-leak)

Your browser's website login presence fingerprint **is not unique**! We found 45 collision(s) among the 17275 browsers tested so far!

59/59

Social mediums where you seem to be logged into:

Website	Detection method
Youtube	Redirection URL hijacking (check it here)
Gmail	Redirection URL hijacking (check it here)
Twitter	Redirection URL hijacking (check it here)