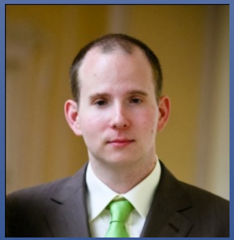
Browser Extension and Login-Leak Experiment

IPEN 2017, Vienna
Joint work with Nataliia Bielova, Claude Castelluccia

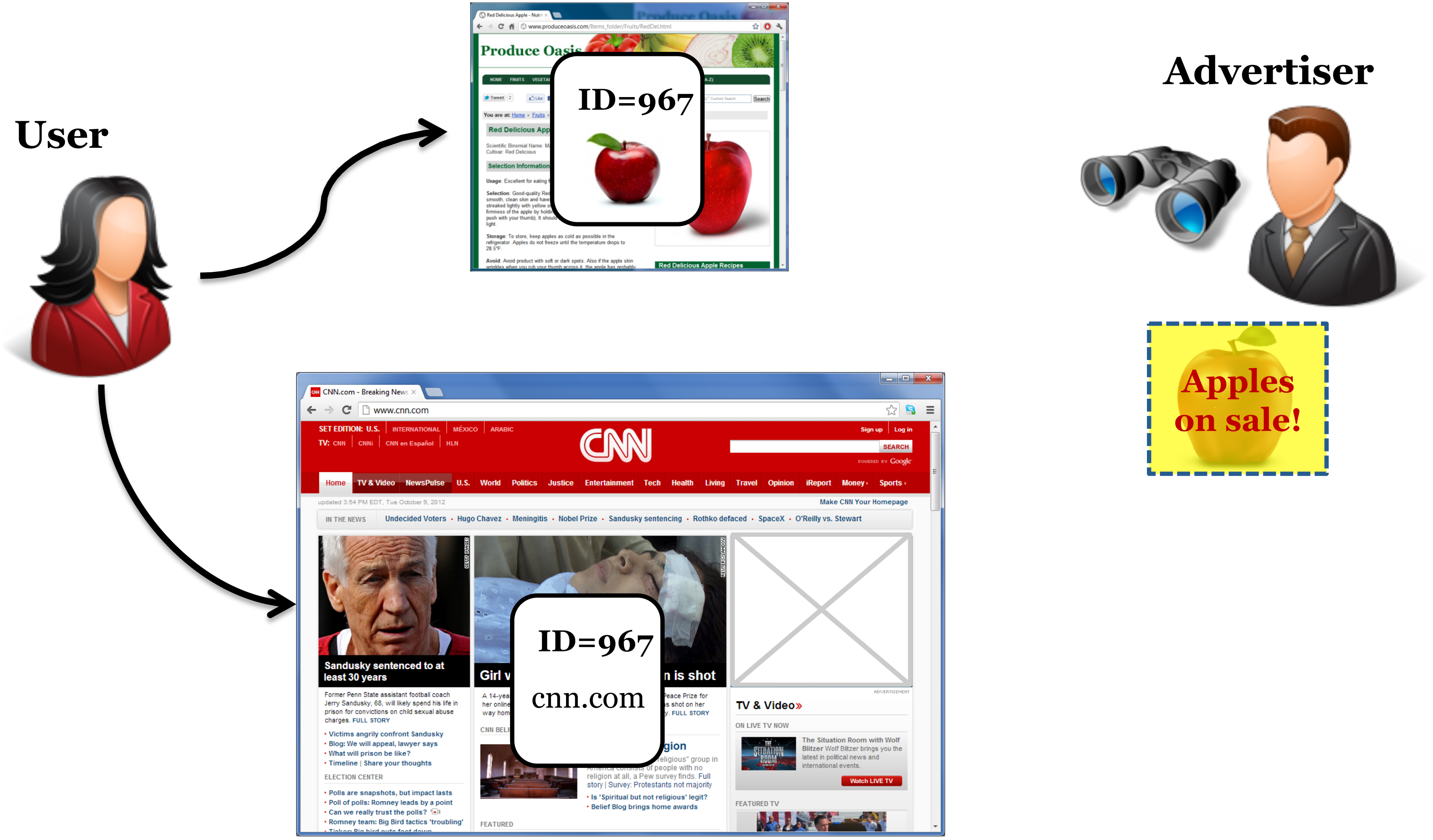
Gábor György Gulyás
Privatics Team, INRIA
http://gulyas.info // @GulyasGG



Inria
INVENTEURS DU MONDE NUMÉRIQUE

User Tracking on the Web

The „de-facto” busniess model of the web



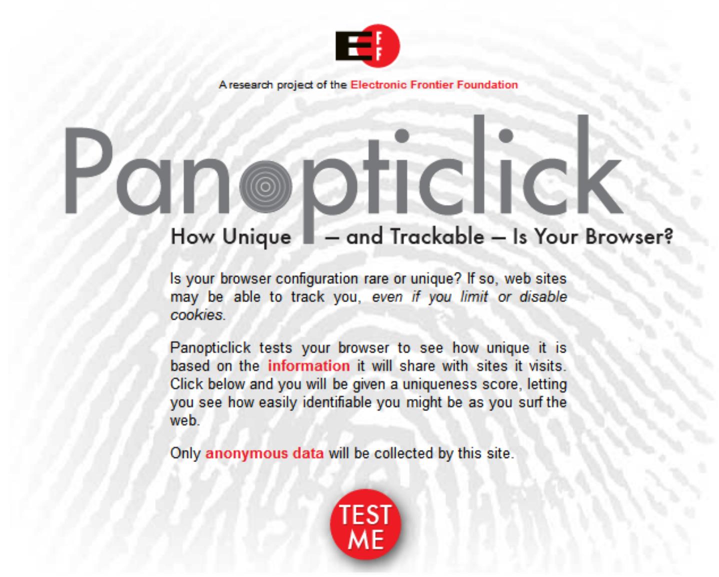
Storing the identifier on the client side

- Cookies
  - Flash
  - HTML5
- Caching in files of
  - JavaScript
  - CSS
  - Images (pixel-level)

- E-tags
- Last-mod timestamps
- HTTP authentication
- HTTP 301 redirect
- HSTS caches

…

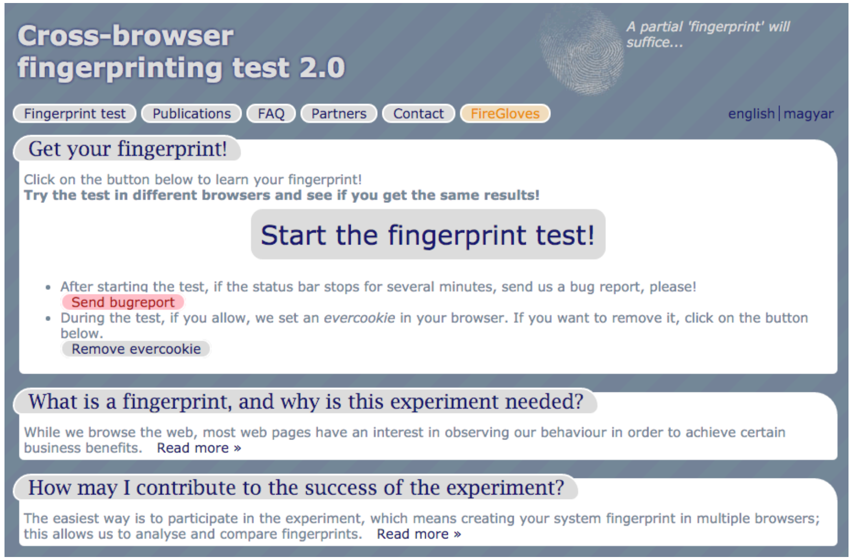
Browser fingerprinting appears (2010-2012) [3]


A research project of the Electronic Frontier Foundation
Panopticlick
How Unique — and Trackable — Is Your Browser?
TEST ME

Is your browser configuration rare or unique? If so, web sites may be able to track you, *even if you limit or disable cookies.*

Panopticlick tests your browser to see how unique it is based on the information it will share with sites it visits. Click below and you will be given a uniqueness score, letting you see how easily identifiable you might be as you surf the web.

Only anonymous data will be collected by this site.


Cross-browser fingerprinting test 2.0
A partial 'fingerprint' will suffice...
Fingerprint test
Publications
FAQ
Partners
Contact
FireGloves
english | magyar
Start the fingerprint test!
Send bugreport
Remove evercookie

Get your fingerprint!

Click on the button below to learn your fingerprint!
Try the test in different browsers and see if you get the same results!

- After starting the test, if the status bar stops for several minutes, send us a bug report, please!
- During the test, if you allow, we set an *evercookie* in your browser. If you want to remove it, click on the button below.

What is a fingerprint, and why is this experiment needed?

While we browse the web, most web pages have an interest in observing our behaviour in order to achieve certain business benefits. Read more »

How may I contribute to the success of the experiment?

The easiest way is to participate in the experiment, which means creating your system fingerprint in multiple browsers; this allows us to analyse and compare fingerprints. Read more »

http://panopticlick.eff.org

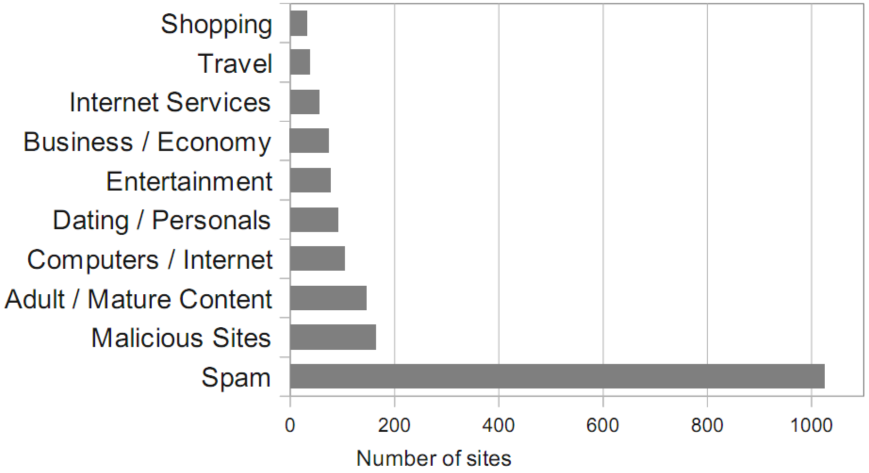
https://fingerprint.pet-portal.eu

- Browser fingerprint
  - Flash/Java required (for 95% uniqueness)
  - Browser dependent
- Cross-browser fingp.
  - Device fingerprint
  - No plugins, just JS
  - Concept appears later in the wild

Fingerprinting penetration (2013-2016)

2013: Alexa TOP 10k.

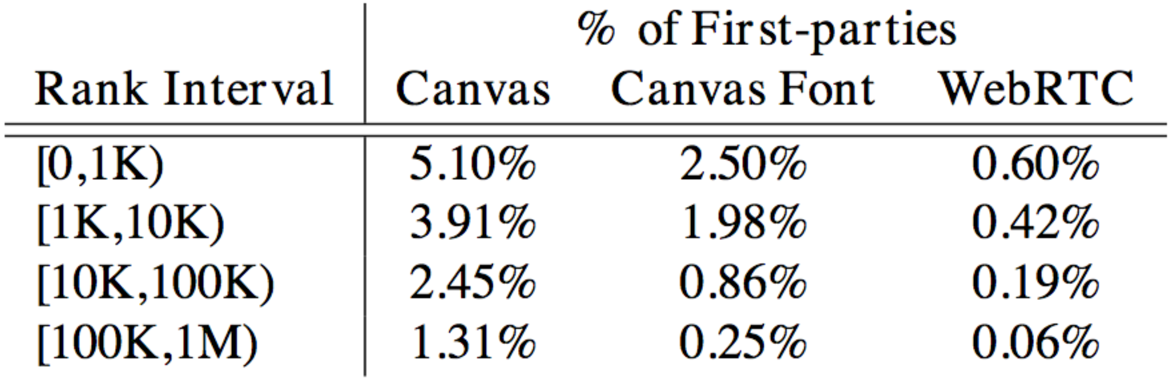
- 20 pages deep
- 0,4% adoption (40 sites)
- Skype.com, porn and dating
- 3 804 less popular sites are tracked



Nickiforakis et al.: Cookieless monster: Exploring the ecosystem of web-based device fingerprinting (2013)

2016: Alexa TOP 1M.

Cwm fjordbank glyphs vext q
Cwm fjordbank gl



	% of First-parties		
Rank Interval	Canvas	Canvas Font	WebRTC
[0,1K)	5.10%	2.50%	0.60%
[1K,10K)	3.91%	1.98%	0.42%
[10K,100K)	2.45%	0.86%	0.19%
[100K,1M)	1.31%	0.25%	0.06%

S. Englehardt, A. Narayanan: Online tracking: A 1-illion-site measurement and analysis (2016)

Behavioral fingerprinting

You are what you install to you computer?

Fonts are good indicators of what is installed.

Boda et al.: User Tracking on the Web via Cross-Browser Fingerprinting (2011)

Google.com Youtube.com
Facebook.com Baidu.com
Yahoo.com Wikipedia.org
Google.co.in Qq.com Sohu.com
Google.co.jp Taobao.com
Tmall.com Live.com Amazon.com
Vk.com Twitter.com
Instagram.com 360.cn

The list of the sites you have visited also describe you well.

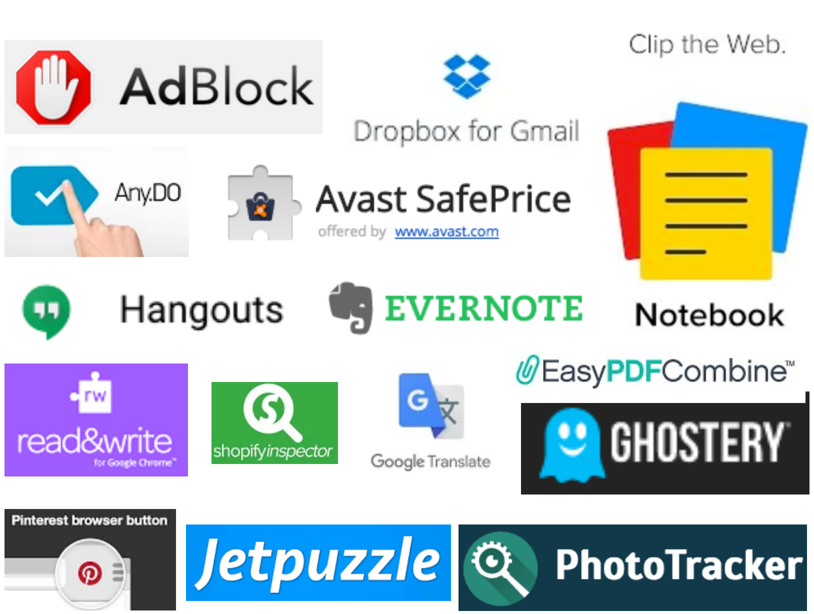
Can be used to de-anonymize you as a natural person.

Su et al.: De-anonymizing Web Browsing Data with Social Networks (2017)

Browser Extension and Login-Leak Experiment

Browser Extension and Login-Leak Experiment

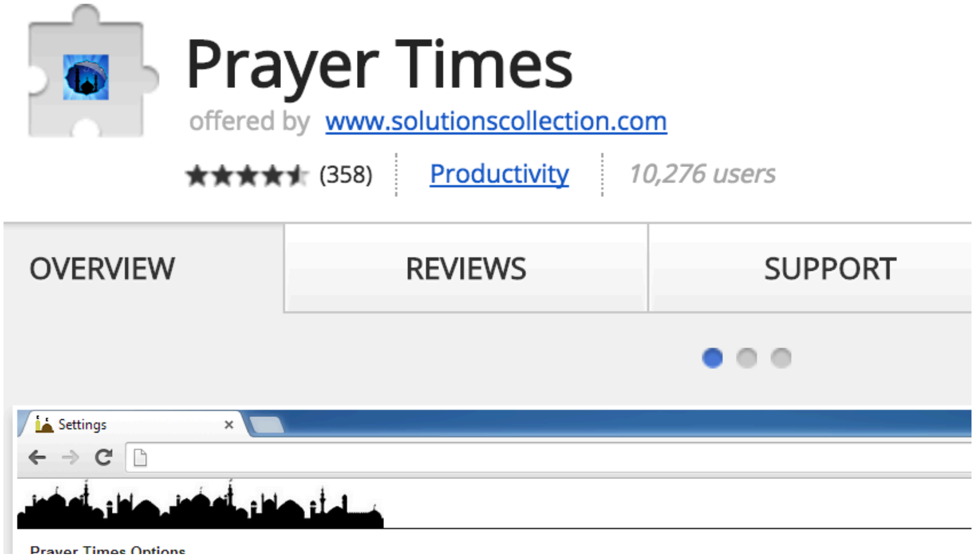
- Extension detection
  - Detecting extension resources
- Detecting web logins
  - Redirection URL hijacking
  - Misusing CSP violation



twitter
YouTube
skype
Pinterest
flickr
EVERNOTE
Meetup
Spotify
PayPal
Y
amazon
airbnb
GitHub
Bitbucket
Dropbox
Academia.edu
inria
informatics mathematics

Why is this a problem?

Extensions can **leak private information**!



Prayer Times

offered by www.solutionscollection.com

★★★★½ (358) | Productivity | 10,276 users

OVERVIEW | REVIEWS | SUPPORT

Settings

Prayer Times Options

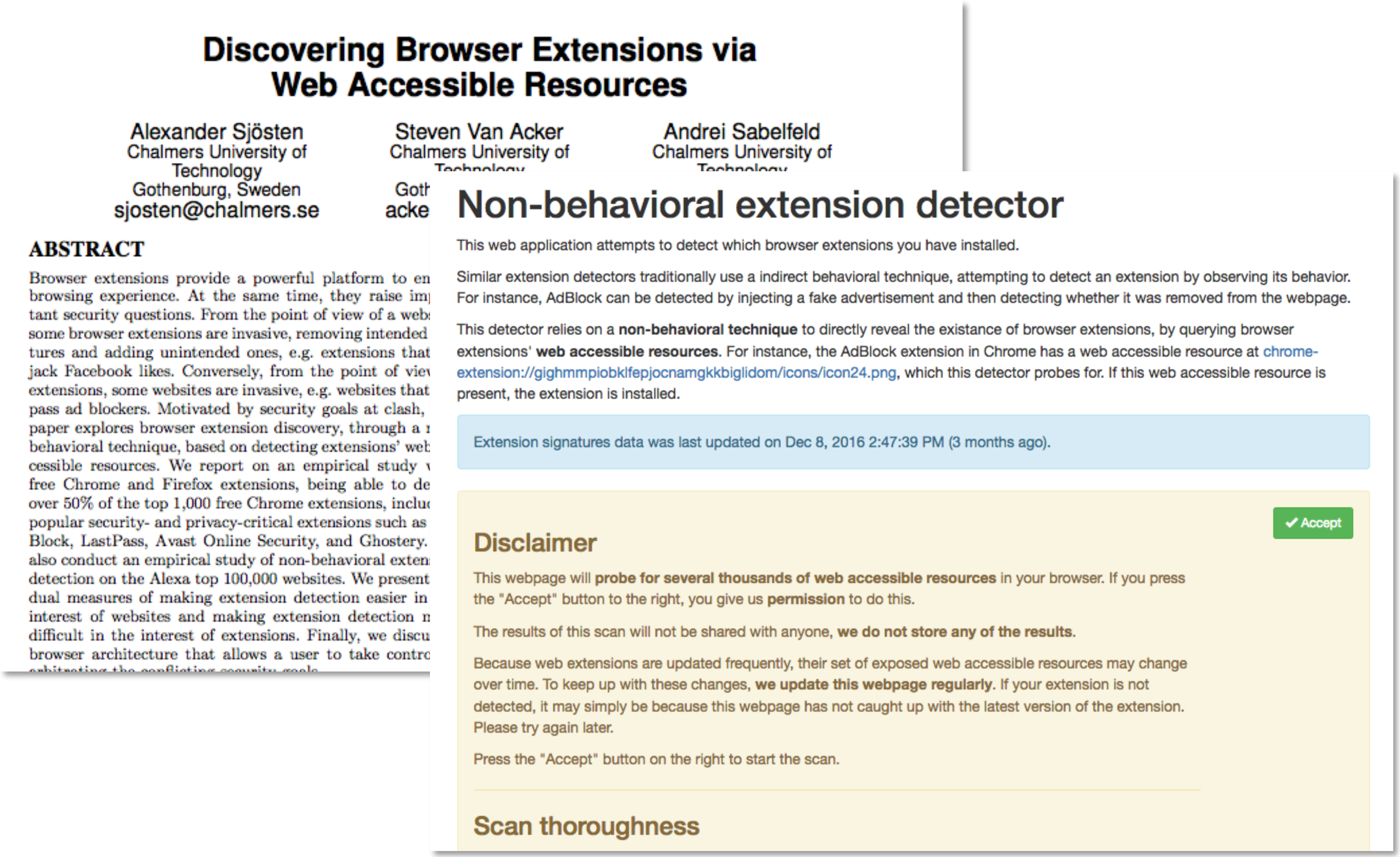
AdBlock

DISCONNECT

GHOSTERY

The more privacy extensions you install, the **more identifiable you are**!

Extension detection history



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
Goth
acke

Andrei Sabelfeld
Chalmers University of
Technology

ABSTRACT

Browser extensions provide a powerful platform to en
browsing experience. At the same time, they raise im
tant security questions. From the point of view of a web
some browser extensions are invasive, removing intended
tures and adding unintended ones, e.g. extensions that
jack Facebook likes. Conversely, from the point of vie
extensions, some websites are invasive, e.g. websites that
pass ad blockers. Motivated by security goals at clash,
paper explores browser extension discovery, through a
behavioral technique, based on detecting extensions' web
cessible resources. We report on an empirical study
free Chrome and Firefox extensions, being able to de
over 50% of the top 1,000 free Chrome extensions, inclu
popular security- and privacy-critical extensions such as
Block, LastPass, Avast Online Security, and Ghostery.
also conduct an empirical study of non-behavioral exten
detection on the Alexa top 100,000 websites. We present
dual measures of making extension detection easier in
interest of websites and making extension detection
difficult in the interest of extensions. Finally, we discu
browser architecture that allows a user to take contro
arbitrating the conflicting security goals

Non-behavioral extension detector

This web application attempts to detect which browser extensions you have installed.

Similar extension detectors traditionally use a indirect behavioral technique, attempting to detect an extension by observing its behavior. For instance, AdBlock can be detected by injecting a fake advertisement and then detecting whether it was removed from the webpage.

This detector relies on a **non-behavioral technique** to directly reveal the existance of browser extensions, by querying browser extensions' **web accessible resources**. For instance, the AdBlock extension in Chrome has a web accessible resource at chrome-extension://gighmmpiobklfepjocnamgkkbiglidom/icons/icon24.png, which this detector probes for. If this web accessible resource is present, the extension is installed.

Extension signatures data was last updated on Dec 8, 2016 2:47:39 PM (3 months ago).

Disclaimer

This webpage will **probe for several thousands of web accessible resources** in your browser. If you press the "Accept" button to the right, you give us **permission** to do this.

The results of this scan will not be shared with anyone, **we do not store any of the results.**

Because web extensions are updated frequently, their set of exposed web accessible resources may change over time. To keep up with these changes, **we update this webpage regularly**. If your extension is not detected, it may simply be because this webpage has not caught up with the latest version of the extension. Please try again later.

Press the "Accept" button on the right to start the scan.

Scan thoroughness

How does it work?

chrome-extension://mlomiejdfkolichcflejclcbmpeaniij/app/images/apps_pages/tracker.png

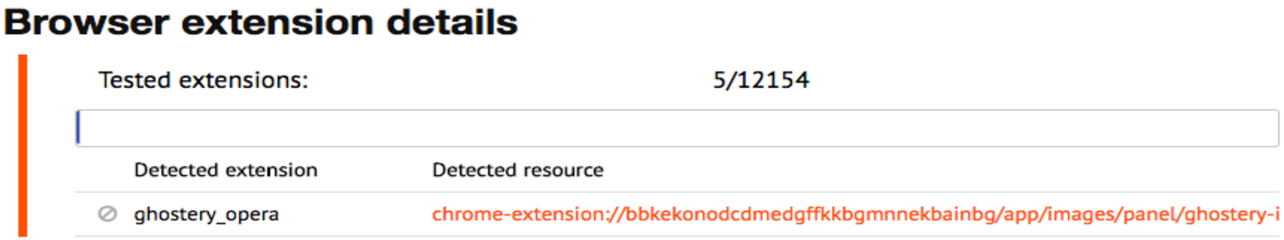
Extension ID (Ghostery)

Local filepath

- Try yourself: http://tinyurl.com/chrome-ghostery
- High precision & coverage:
  - Large fraction of extensions covered ~28%
  - No false-positives (uninstalled extensions not reported)
- Robustness (multiple resources can be checked)

Other browsers?

- Firefox
  - Smaller impact: ~7% (direct possibility to manipulate UI)
  - WebExtensions ➔ same vulnerability as Chrome (but ~5.5%)
  - Resources leak more information
- Opera



Browser extension details

Tested extensions: 5/12154

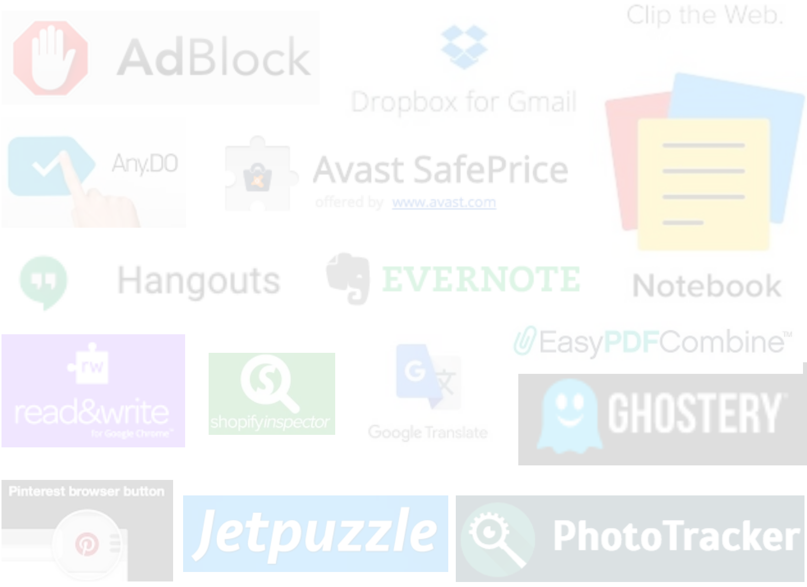
Detected extension	Detected resource
⊘ ghostery_opera	chrome-extension://bbkekonodcdmedgffkkbgmnnekbainbg/app/images/panel/ghostery-i

- Brave
  - Comes with detectable built-in extensions
  - Test it here: https://extensions.inrialpes.fr/brave/
- Edge
  - It is possible [http://tinyurl.com/edge-ext]
  - Low number of extensions are available

Browser Extension and Login-Leak Experiment

- Extension detection
  - Detecting extension resources

- Detecting web logins
  - Redirection URL hijacking
  - Misusing CSP violation



twitter
YouTube
f
skype
Pinterest
flickr
EVERNOTE
Meetup
Spotify
PayPal
Y
amazon
airbnb
GitHub
Bitbucket
Dropbox
Academia.edu
Inria
informatics mathematics

Why is this a problem?

Allows very **precise profiling**.

Leaks **sensitive info (security!)**.

Tells about **where you work**.

Allow **behavioral tracking**.

Currently detected sites (60)

Social & Fun

- Battle.net
- Facebook
- Flickr
- Foursquare
- Gmail
- Google Plus
- Instagram
- LinkedIn
- Meetup
- Pinterest
- Skype
- Spotify
- Tumblr
- Twitter
- VK
- Youtube

Shopping

- 500px
- Alibaba.com, Aliexpress.com
- Airbnb
- Amazon.{co.uk, com, de, fr, it}
- eBay.{co.uk, com, de, fr, it}
- Expedia
- Paypal
- Photobucket
- shutterstock
- Steam
- Square

Gray zone

- Youporn
- Dating sites

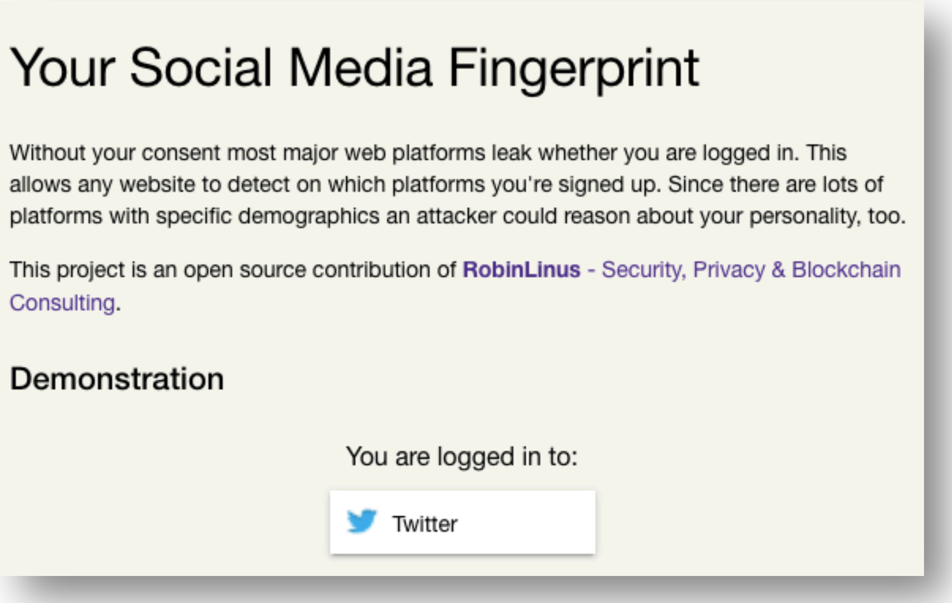
News & Blogging

- Forbes
- Hackernews
- LeMonde.fr
- LiveJournal
- Medium
- Reddit
- Spiegel.de
- Yahoo

Work & Education

- Academia.edu
- BitBucket
- Carbonmade
- Dropbox
- EdX
- Evernote
- Github
- Indeed
- Inria
- Khan Academy
- PluralSight
- Scribd
- Slack
- SugarSync
- Viadeo

Techniques used



Your Social Media Fingerprint

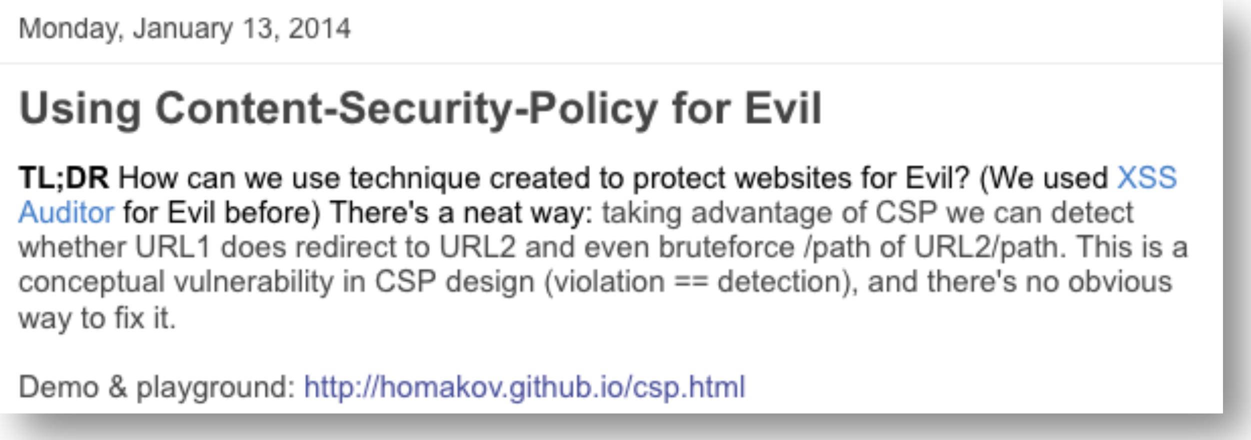
Without your consent most major web platforms leak whether you are logged in. This allows any website to detect on which platforms you're signed up. Since there are lots of platforms with specific demographics an attacker could reason about your personality, too.

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

Demonstration

You are logged in to:

Redirection URL hijacking
by [@robin_linus]



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

Abusing Content
Security Policy
by @homakov

How do they work?

Redirection URL hijacking

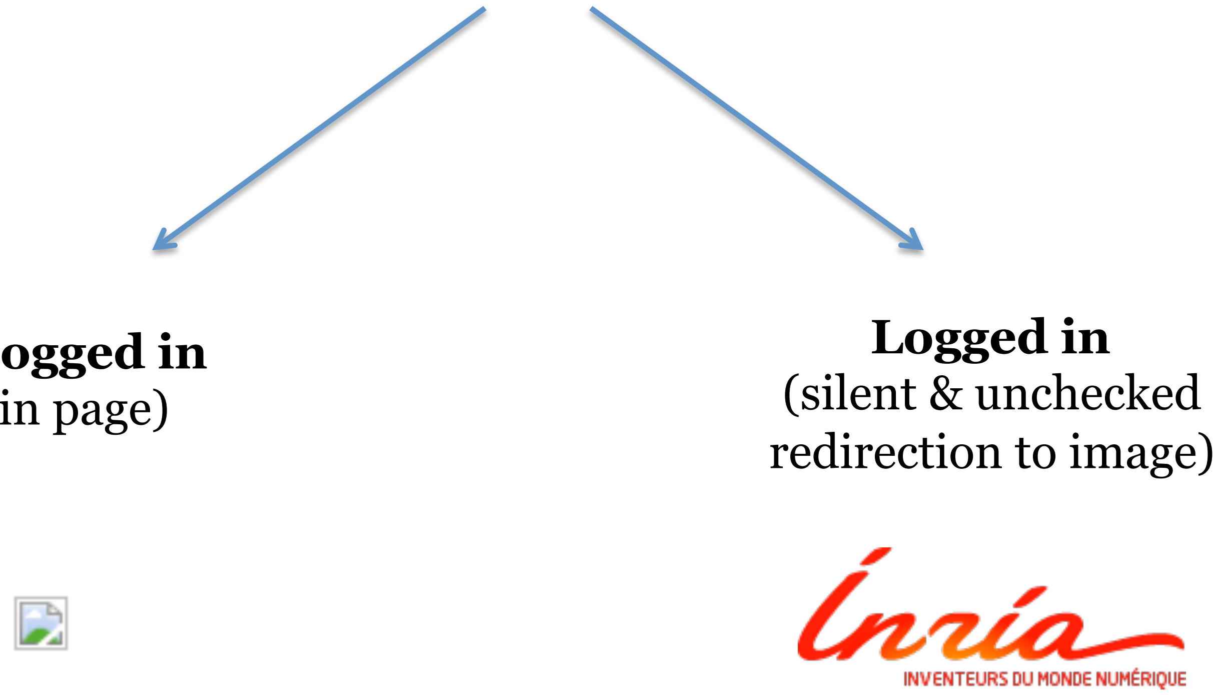
```
https://inria.fr/login?return=CALENDAR
```

How do they work? [2]

Redirection URL hijacking

`<img />`

```
https://inria.fr/login?return=logo_INRIA.png
```

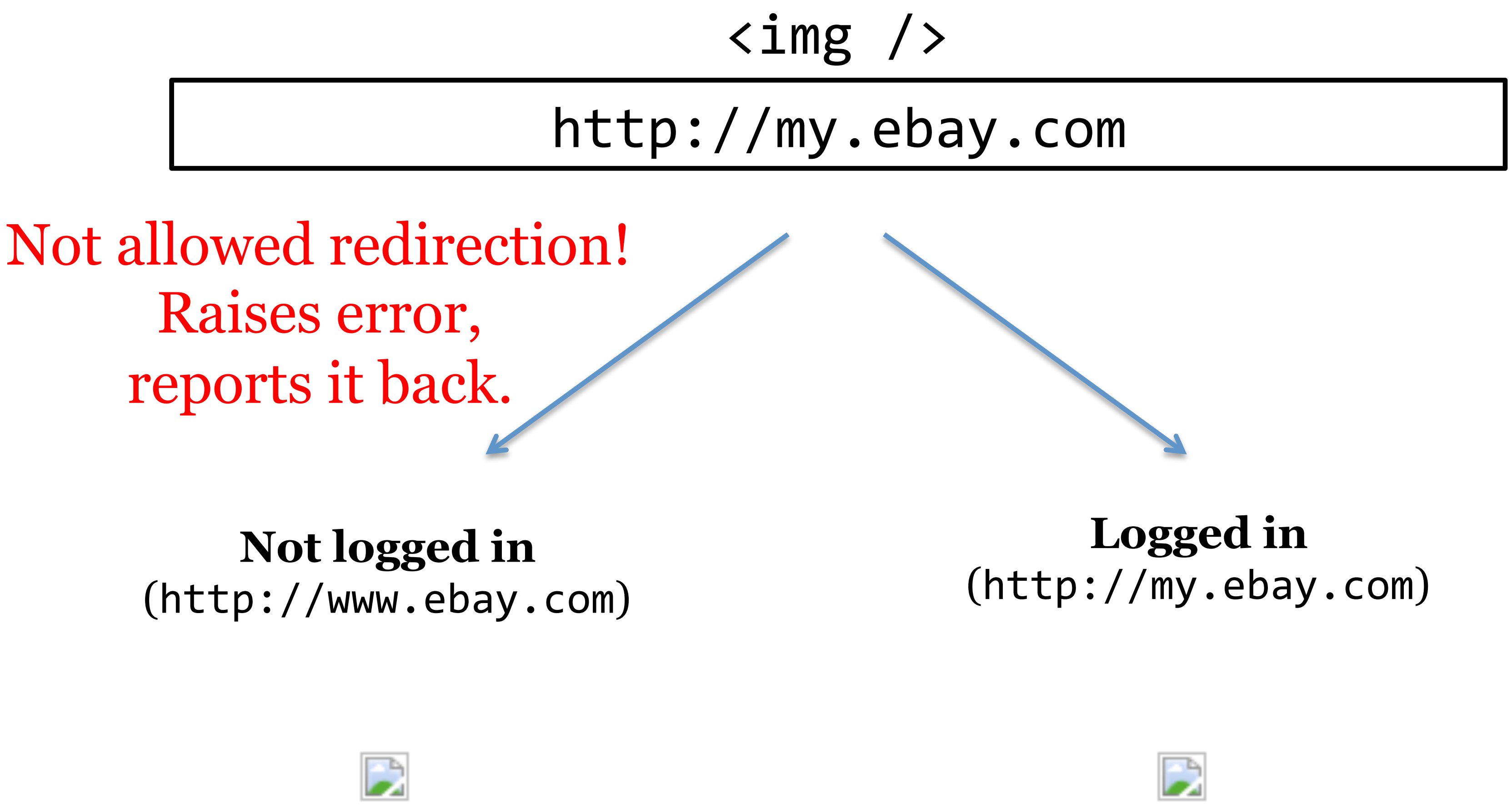


Not logged in
(login page)

Logged in
(silent & unchecked
redirection to image)

How do they work? [3]

Abusing CSP



`<img />`

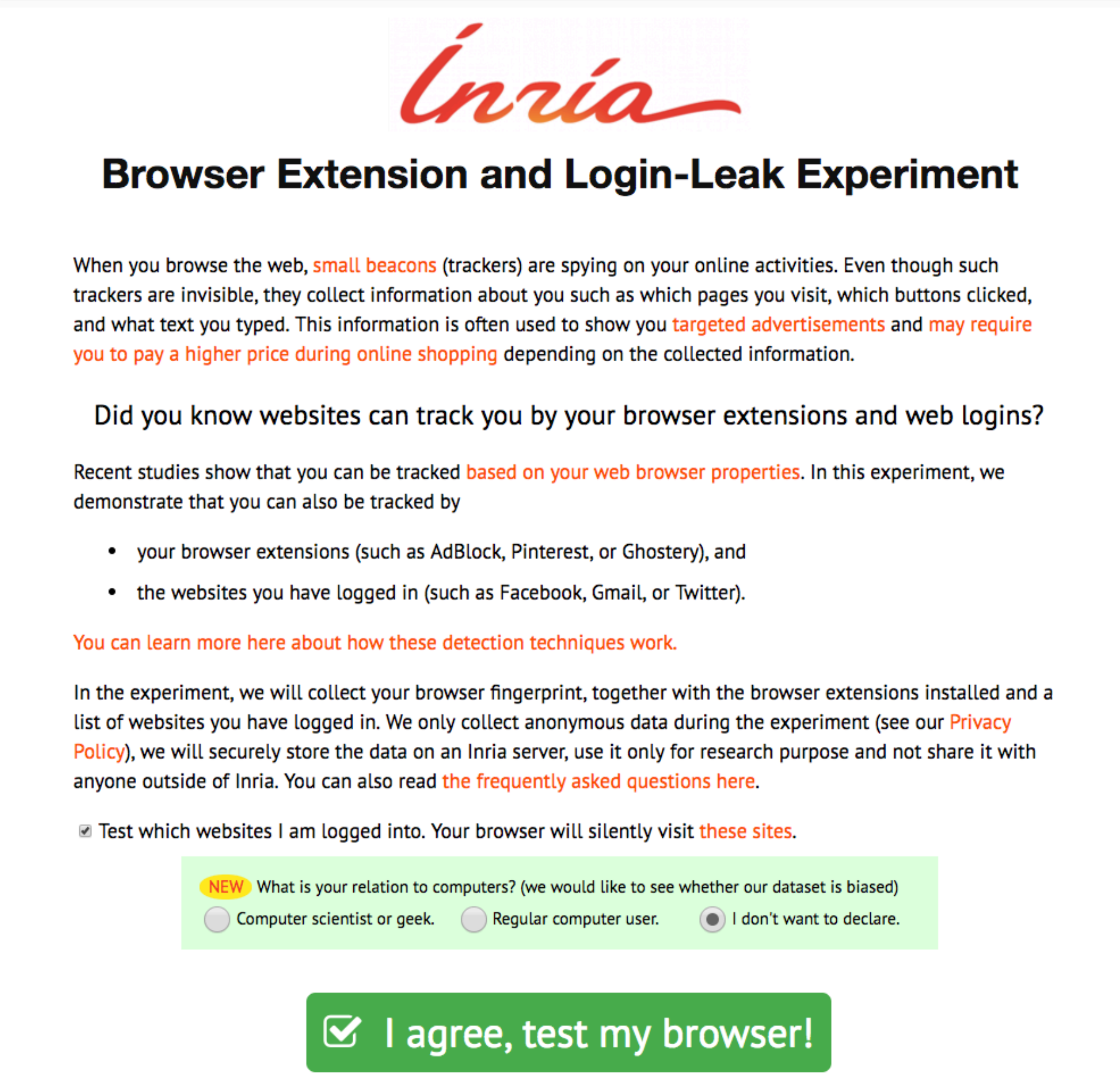
`http://my.ebay.com`

Not allowed redirection!
Raises error,
reports it back.

Not logged in
(`http://www.ebay.com`)

Logged in
(`http://my.ebay.com`)

https://extensions.inrialpes.fr



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.

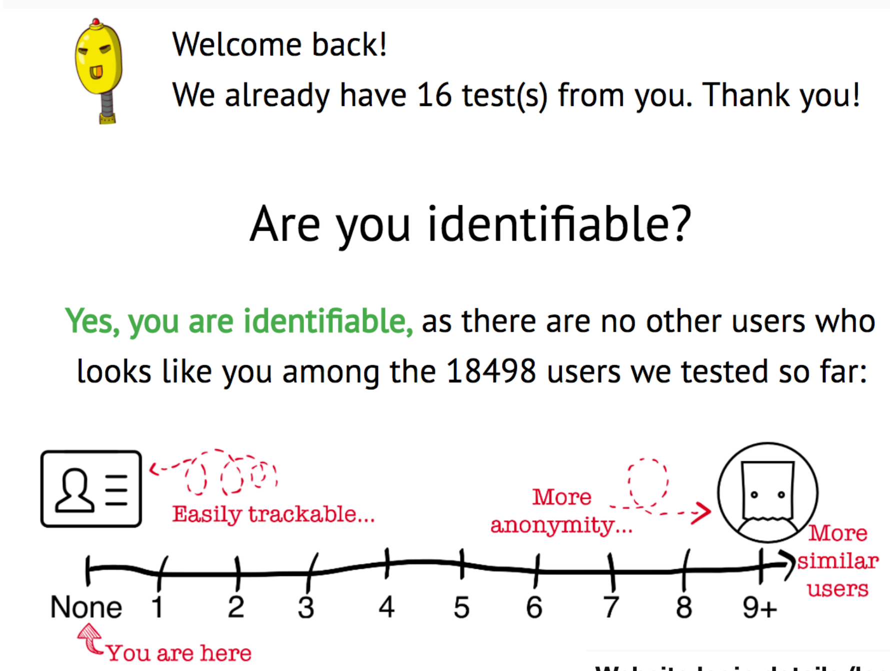
In the experiment, we will collect your browser fingerprint, together with the browser extensions installed and a list of websites you have logged in. We only collect anonymous data during the experiment (see our Privacy Policy), we will securely store the data on an Inria server, use it only for research purpose and not share it with anyone outside of Inria. You can also read the frequently asked questions here.

☑ Test which websites I am logged into. Your browser will silently visit these sites.

NEW What is your relation to computers? (we would like to see whether our dataset is biased)
○ Computer scientist or geek. ○ Regular computer user. ● I don't want to declare.

☑ I agree, test my browser!

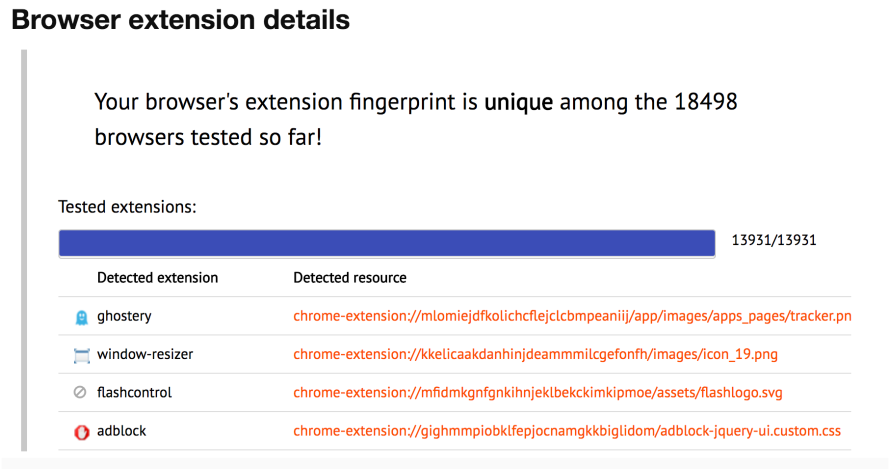
https://extensions.inrialpes.fr



Welcome back!
We already have 16 test(s) from you. Thank you!

Are you identifiable?

Yes, you are identifiable, as there are no other users who looks like you among the 18498 users we tested so far:



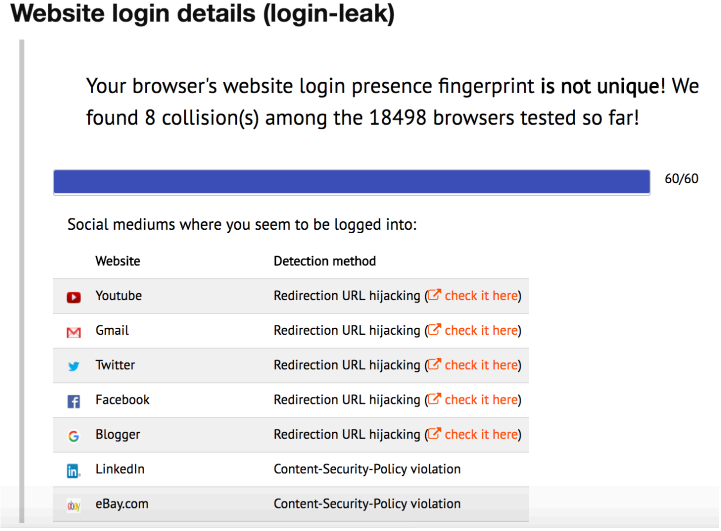
Browser extension details

Your browser's extension fingerprint is **unique** among the 18498 browsers tested so far!

Tested extensions:

13931/13931

Detected extension	Detected resource
ghostery	chrome-extension://mlomiejdfkolichcflejclcbmpeaniij/app/images/apps_pages/tracker.pn
window-resizer	chrome-extension://kkelicaakdanhinjdeammmilcgefonfh/images/icon_19.png
flashcontrol	chrome-extension://mfidmkgnfgnkihnjeklbekckimkipmoe/assets/flashlogo.svg
adblock	chrome-extension://gighmmpiobklfepjocnamgkkbiglidom/adblock-jquery-ui.custom.css



Website login details (login-leak)

Your browser's website login presence fingerprint **is not unique**! We found 8 collision(s) among the 18498 browsers tested so far!

60/60

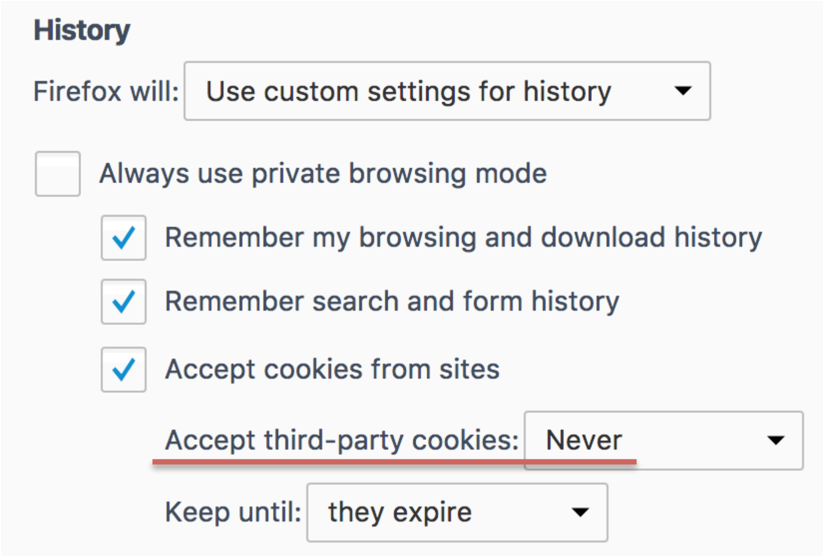
Social mediums where you seem to be logged into:

Website	Detection method
Youtube	Redirection URL hijacking (check it here)
Gmail	Redirection URL hijacking (check it here)
Twitter	Redirection URL hijacking (check it here)
Facebook	Redirection URL hijacking (check it here)
Blogger	Redirection URL hijacking (check it here)
LinkedIn	Content-Security-Policy violation
eBay.com	Content-Security-Policy violation

What could we do (for now)?

Extension detection

- Chrome, Opera, Brave: not much.
- Safari: not evaluated.
- Firefox: vulnerable.
  But: few extensions, and good for privacy.



History

Firefox will: Use custom settings for history

□ Always use private browsing mode

☑ Remember my browsing and download history

☑ Remember search and form history

☑ Accept cookies from sites

Accept third-party cookies: Never

Keep until: they expire

Web login detection

- Best advice is to turn off third-party cookies.
- Or use an extension that blocks
  - access to third-part cookies,
  - tracking, or
  - JavaScript (noscript).

Thank you for your attention!

ANY QUESTIONS?

Gábor György Gulyás
Privatics Team, INRIA
http://gulyas.info // @GulyasGG