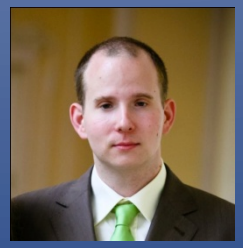
Browser Extension and Login-Leak Experiment

APVP 2017, Vienna

Joint work with Nataliia Bielova, Claude Castelluccia

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

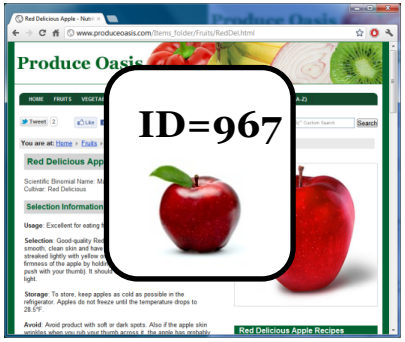


INVENTEURS DU MONDE NUMÉRIQUE

User Tracking on the Web

The „de-facto” business model of the web

User



Advertiser

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]

http://panopticlick.eff.org

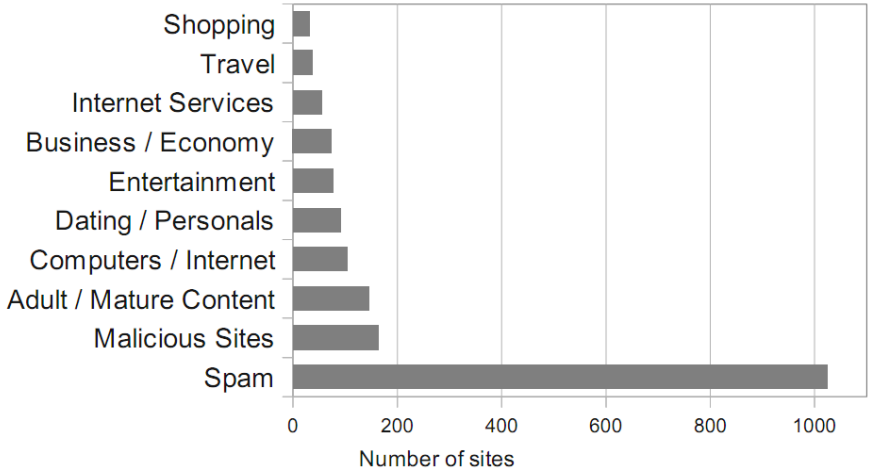
https://fingerprint.pet-portal.eu

- 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.

Rank Interval	% of First-parties		
	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)

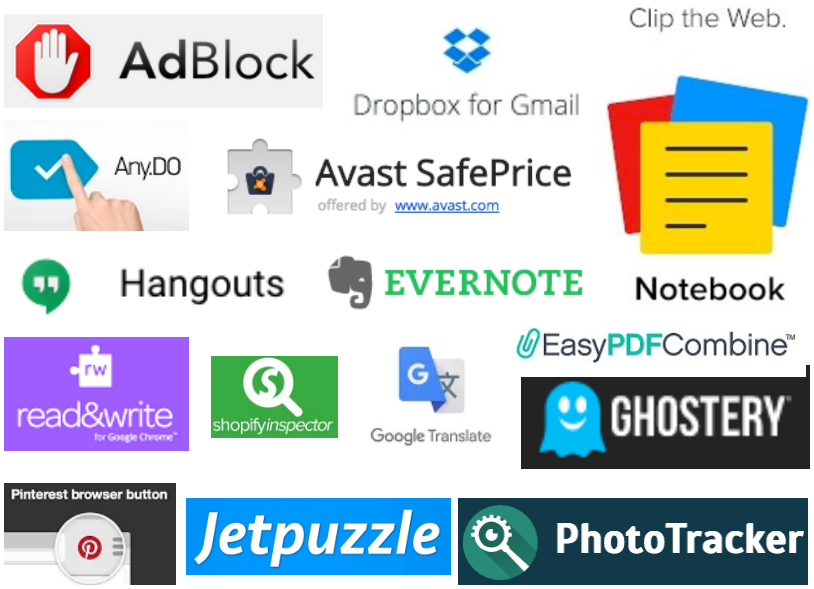
Browser Extension and Login-Leak Experiment

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:

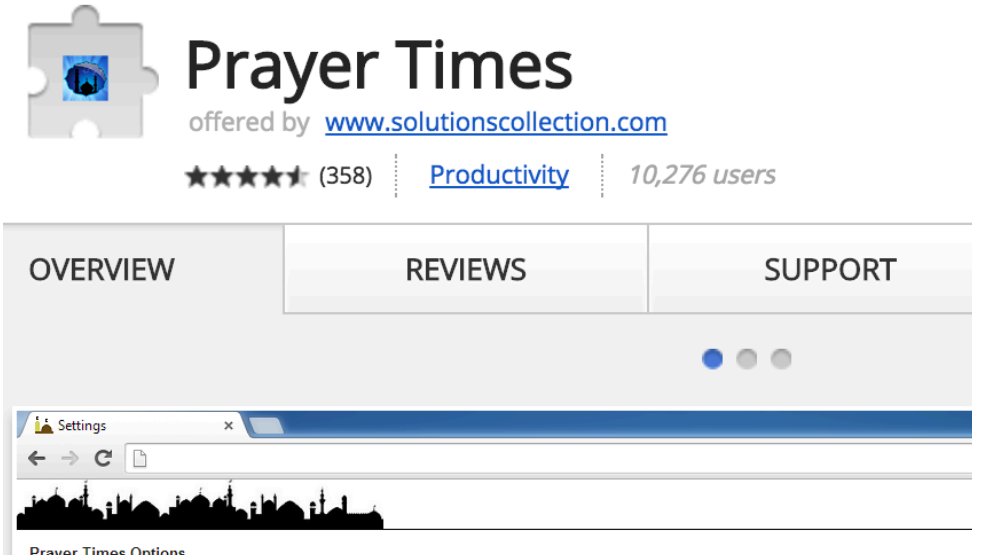
Browser Extension and Login-Leak Experiment

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



Why is this a problem?

Extensions can **leak private information**!



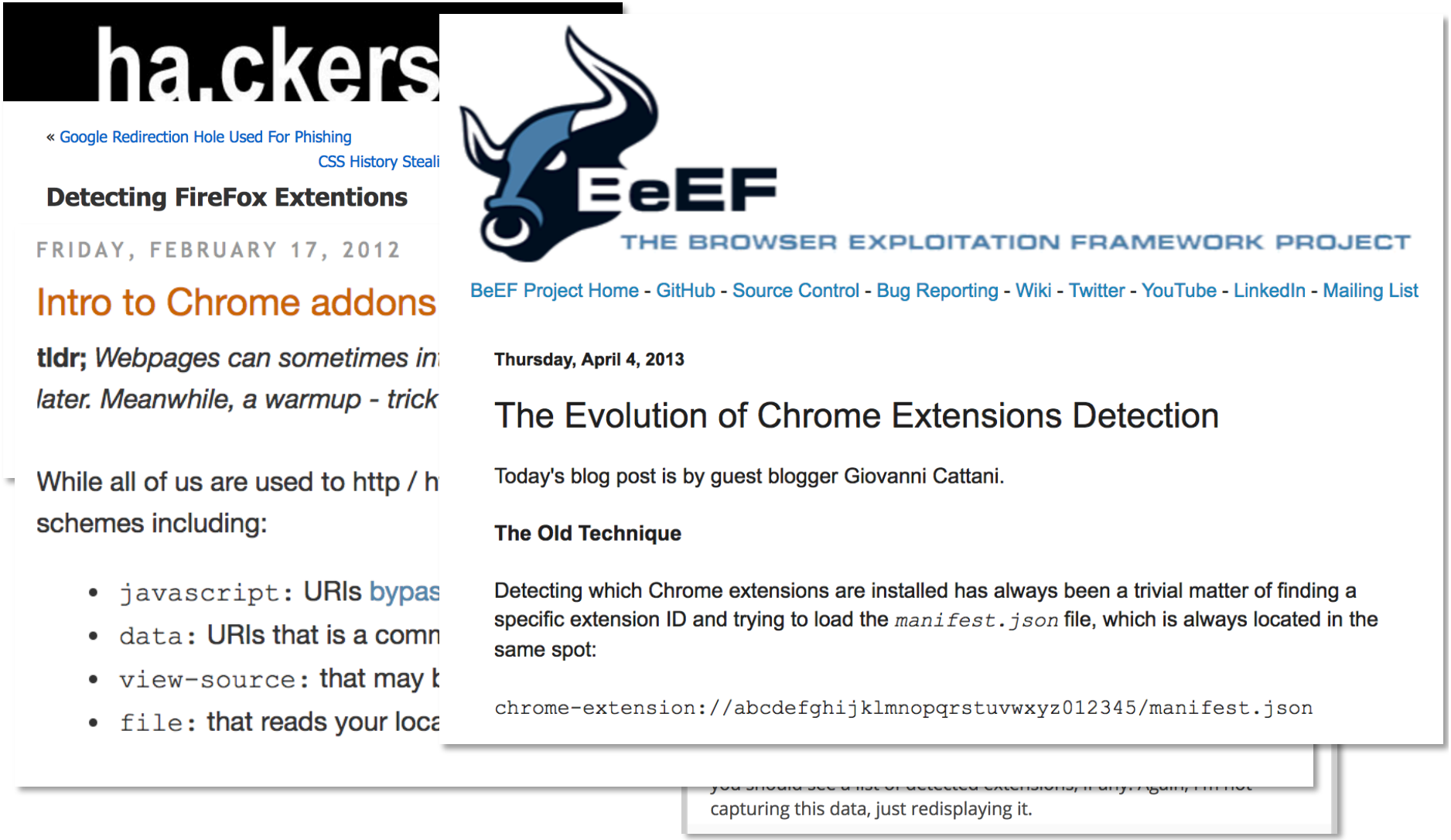
AdBlock

DISCONNECT

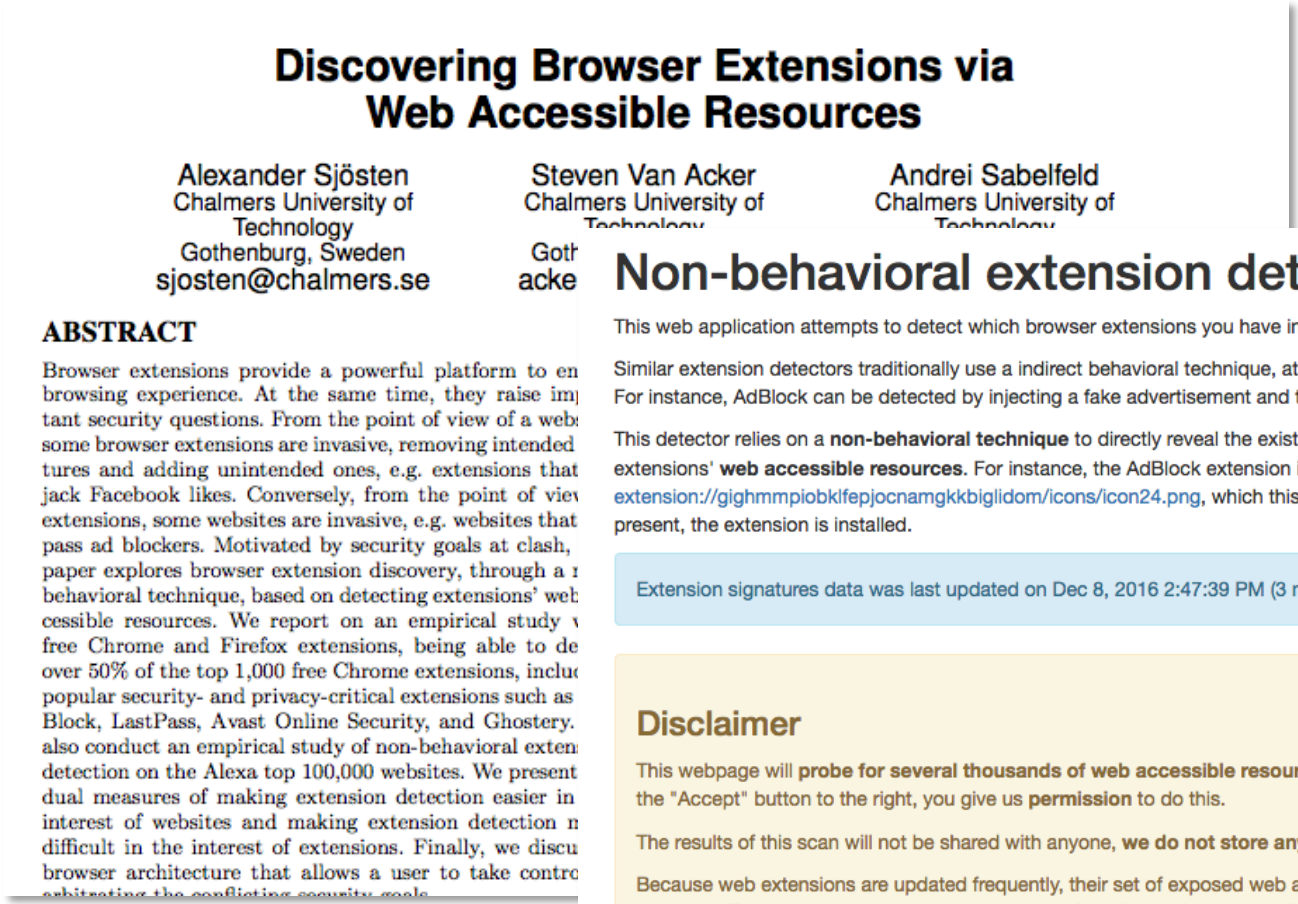
GHOSTERY

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

History of browser extension detection



History of browser extension detection (2)



Discovering Browser Extensions via Web Accessible Resources

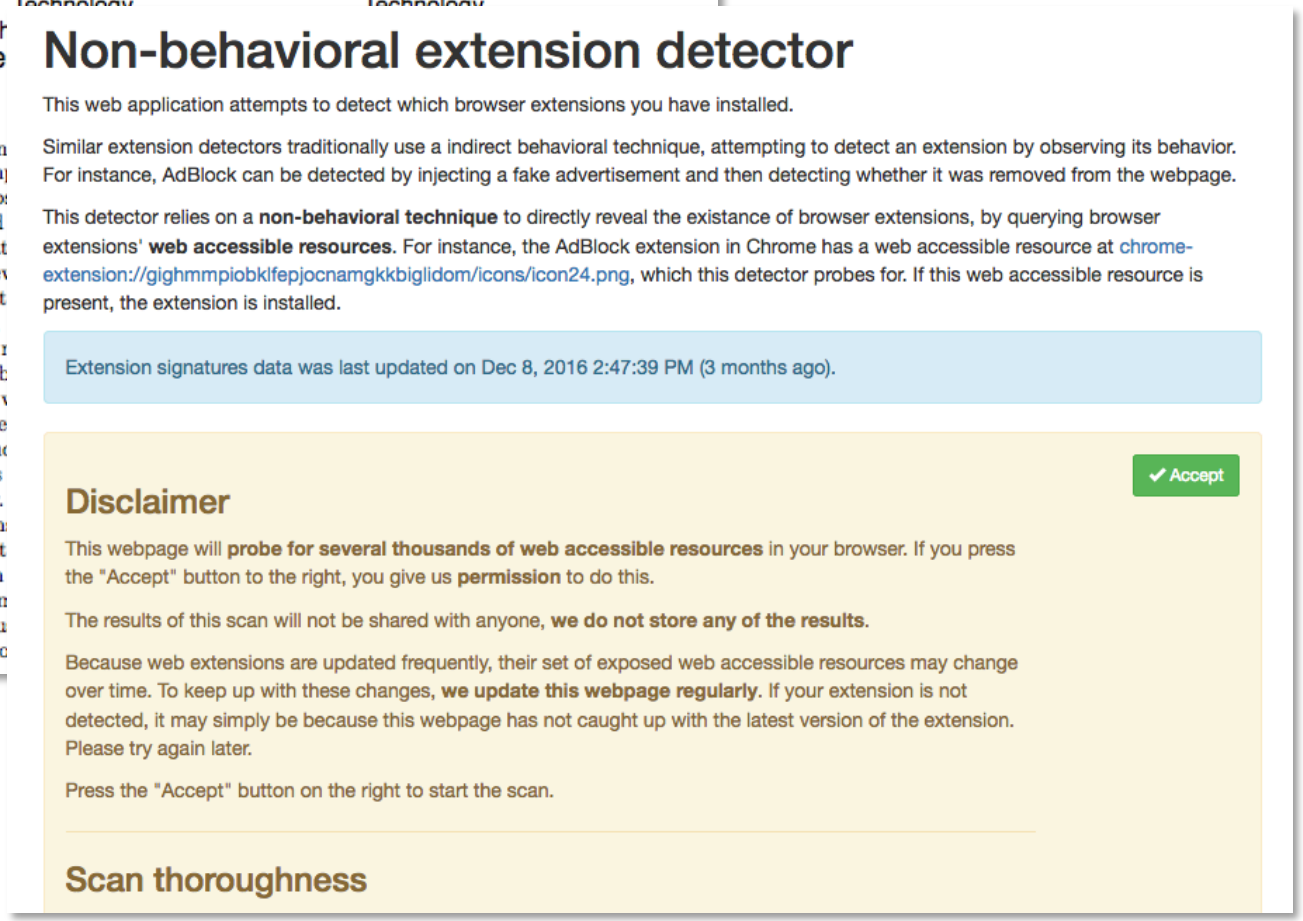
Alexander Sjösten
Chalmers University of Technology
Gothenburg, Sweden
sjosten@chalmers.se

Steven Van Acker
Chalmers University of Technology

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 view
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



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).

✔ Accept

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% (13 892)
  - 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

Why is this a problem?

Allows very **precise profiling**.

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

Tells about **where you work**.

inventeurs du monde numérique

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

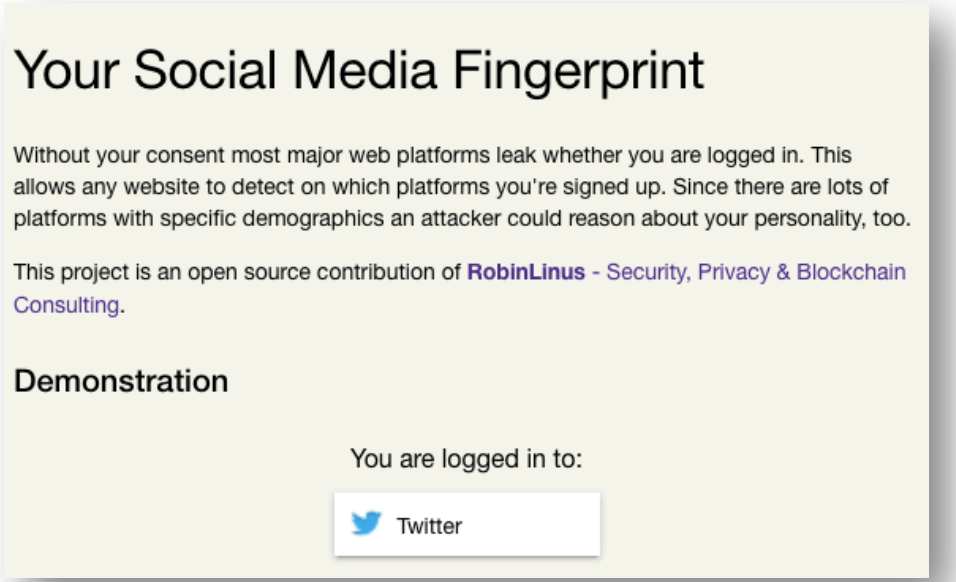
Shopping
- 500px
- Alibaba.com, Aliexpress.com
- Airbnb
- Amazon.{co.uk, com, de, fr, it}
- eBay.{co.uk, com, de, fr, it}
- Expedia
- Paypal
- Photobucket
- shutterstock
- Steam
- Square

Gray zone
- Youporn
- Dating sites

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

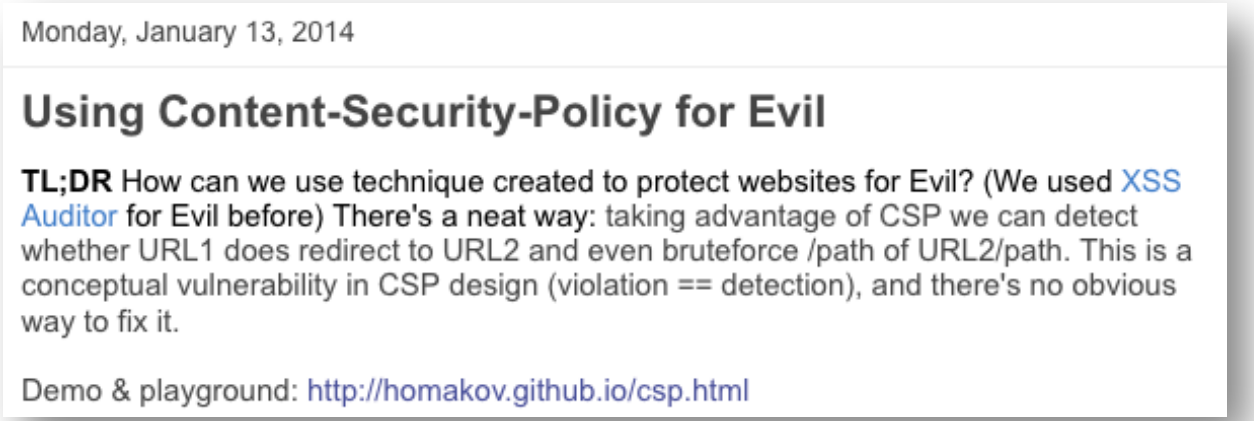
Work & Education
- Academia.edu
- BitBucket
- Carbonmade
- Dropbox
- EdX
- Evernote
- Github
- Indeed
- Inria
- Khan Academy
- PluralSight
- Scribd
- Slack
- SugarSync
- Viadeo

Techniques used



Redirection URL hijacking
by @robin_linus

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 />
```

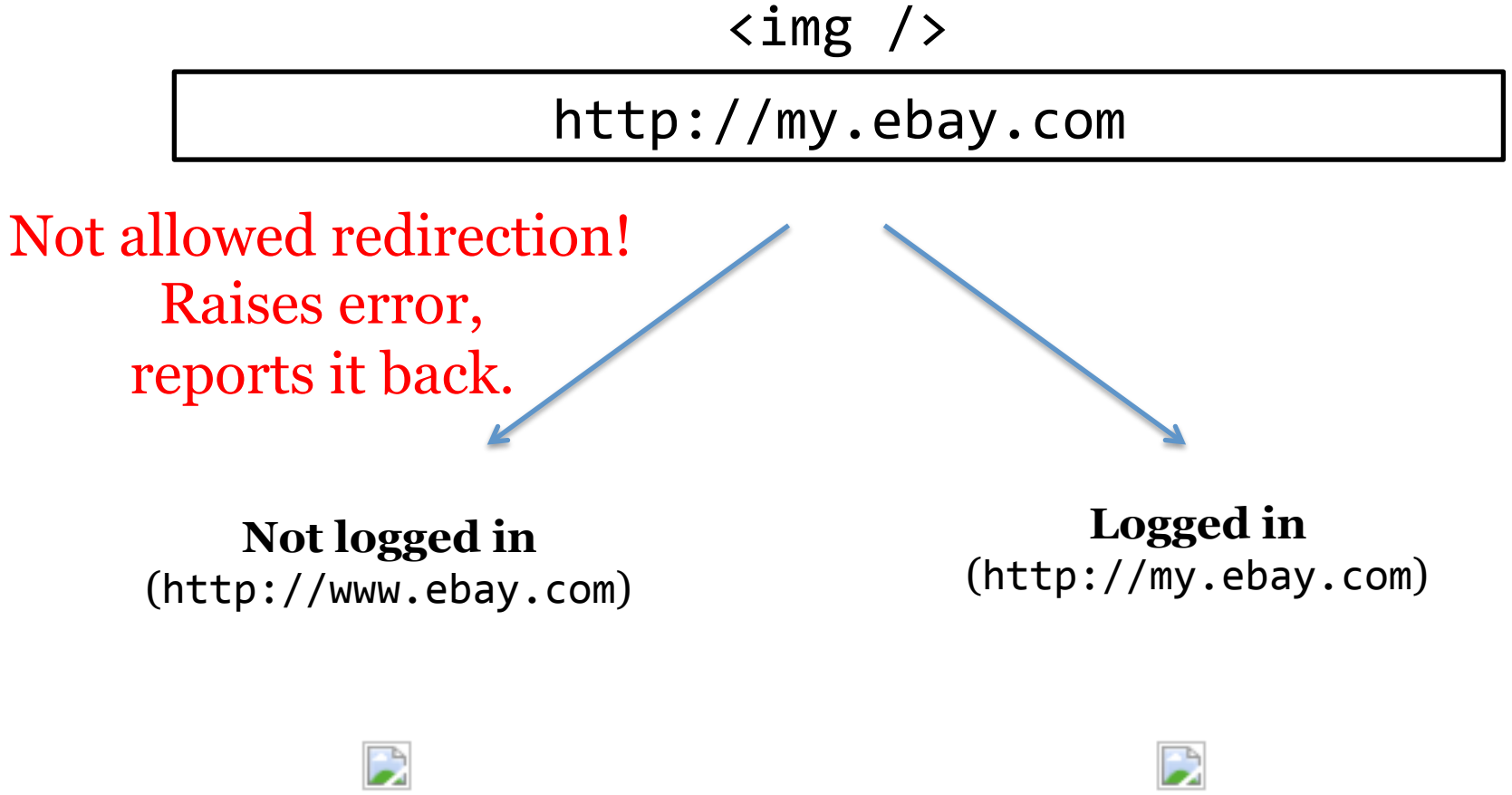
```
https://inria.fr/login?return=logo_INRIA.png
```

Not logged in
(login page)

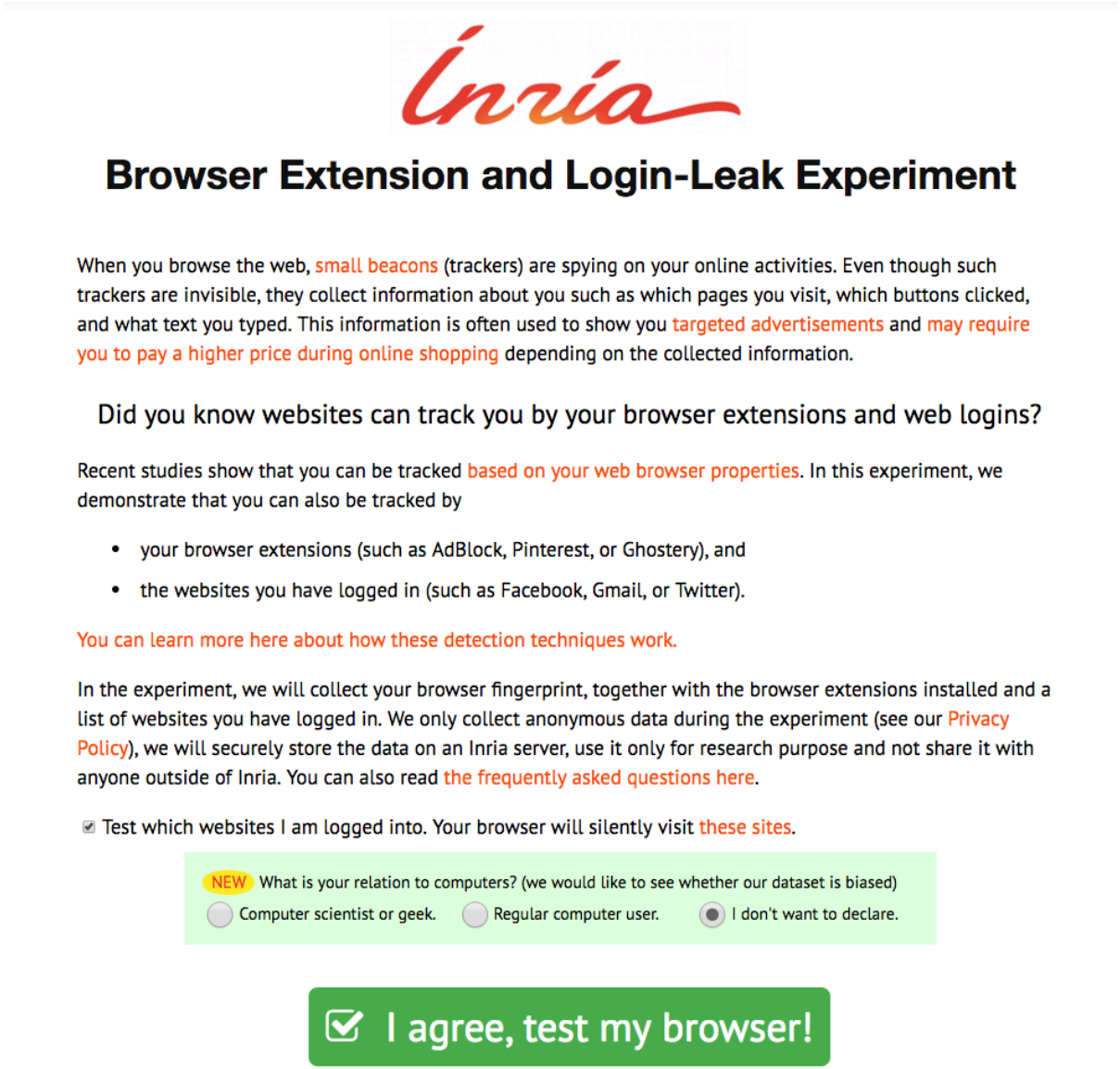
Logged in
(silent & unchecked redirection to image)

How do they work? [3]

Abusing CSP



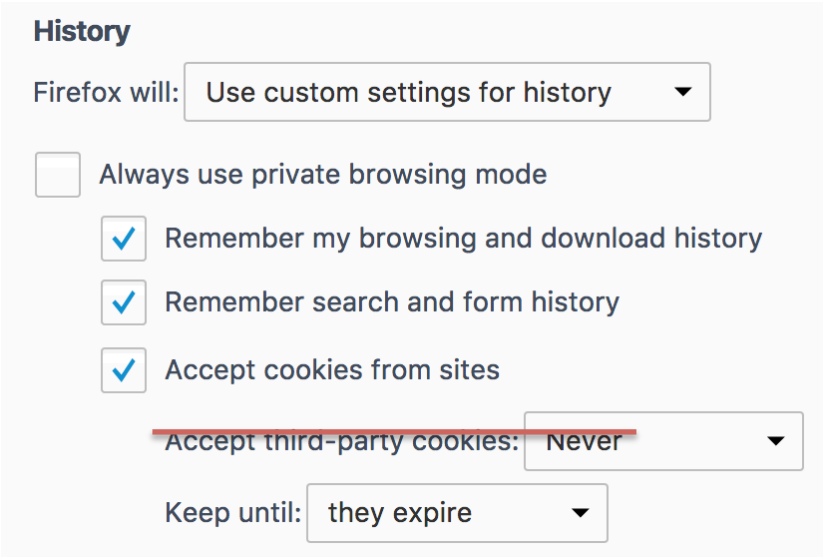
https://extensions.inrialpes.fr



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.



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).

Research issues

- Asses privacy risks posed by these leaks
  - Uniqueness / tracking
  - De-anonymization attacks
  - Security risks
  - …
- Evaluation of extension use and login habits
  - On a wider scale, and also
  - On the personal level (returning visitors)
- Longitudinal study of extensions

Research issues (2)

XHOUND: Quantifying the Fingerprintability of Browser Extensions

Similar roots!

ii Starov
ok University
tonybrook.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

***Abstract*—In recent years, researchers have shown that unwanted web tracking is on the rise, as advertisers are trying to capitalize on users' online activity, using increasingly intrusive and sophisticated techniques. Among these, browser fingerprinting has received the most attention since it allows trackers to uniquely identify users despite the clearing of cookies and the use of a browser's private mode.**

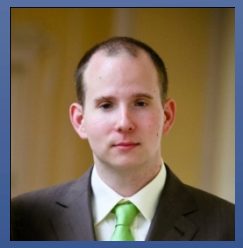
In this paper, we investigate and quantify the fingerprintability of browser extensions, such as, AdBlock and Ghostery. We show that an extension's organic activity in a page's DOM can be used to infer its presence, and develop XHOUND, the first fully automated system for fingerprinting browser extensions. By applying XHOUND to the 10,000 most popular Google Chrome extensions, we find that a significant fraction of popular browser extensions are fingerprintable and could thus be used to sup-

browser plugins remain one of the most revealing features of desktop and laptop browsers, the entropy that they offer has considerably decreased since Eckersley's study. This is due to the increasing popularity of HTML5, providing powerful functionality to developers, and the decreasing trust in proprietary browser plugins which have, in the past, caused many performance and security issues. For instance, Google Chrome has stopped supporting plugins utilizing the NPAPI architecture [3] and Mozilla Firefox announced a plan to do the same [5], while already limiting the ability of scripts to enumerate plugins [1]. As the popularity and fingerprinting power of plugins is decreasing, we argue that trackers will look for new techniques to fingerprint users. Predicting these

Thank you for your attention!

ANY QUESTIONS?

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



INVENTEURS DU MONDE NUMÉRIQUE