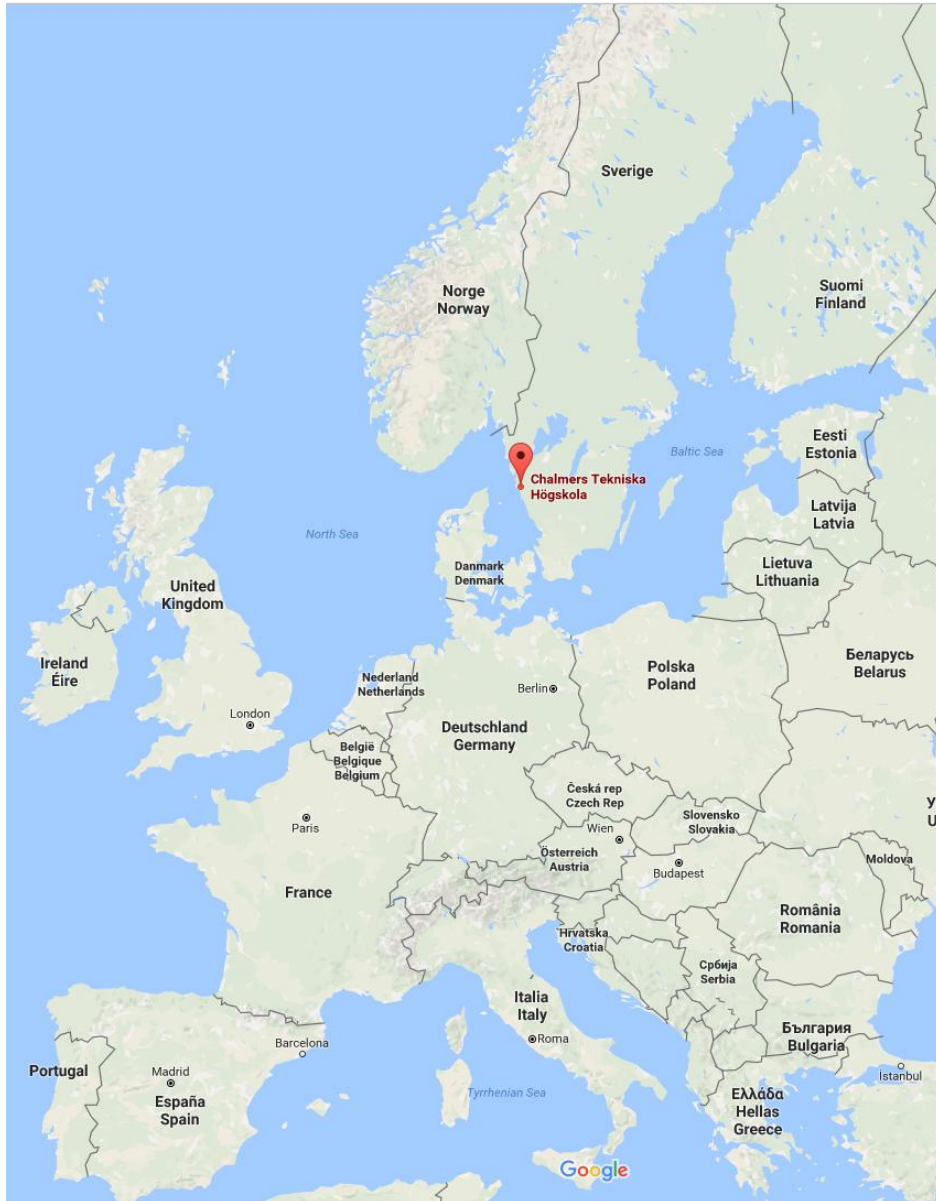


Chalmers University of Technology



The research group

- Supervisor: Professor Andrei Sabelfeld
- 4 PhD students
- 2 postdocs
- 1 Associate Professor at 20%

We do research in

- Web security
- Location Privacy
- Information-Flow Control

Fingerprinting browser extensions with web accessible resources

Alexander Sjösten Steven van Acker Andrei Sabelfeld

Interplay between extensions and webpages

- Play content on a Chromecast
- Streaming sites can add icon when detecting Google Cast
- Cooperation between website and extension
- **Enrich functionality and user experience!**



Goals of websites

- Sensitive information
- Financial interests
 - E.g. ads
- Defensive handling
 - Unwanted modifications
 - Unwanted script injections
- Controlling their own domain
 - Detecting extensions wanted!



Goals of websites

- Over a billion daily users
- Extensions their #1 threat
 - “Like” hijacking
 - Fake content
 - Ad injection
- Malicious extensions pass Chrome webstore vetting
 - Evaded with e.g. dynamic techniques
 - “Free smileys and emoticons”, 1.2M users
- Detecting extensions wanted!

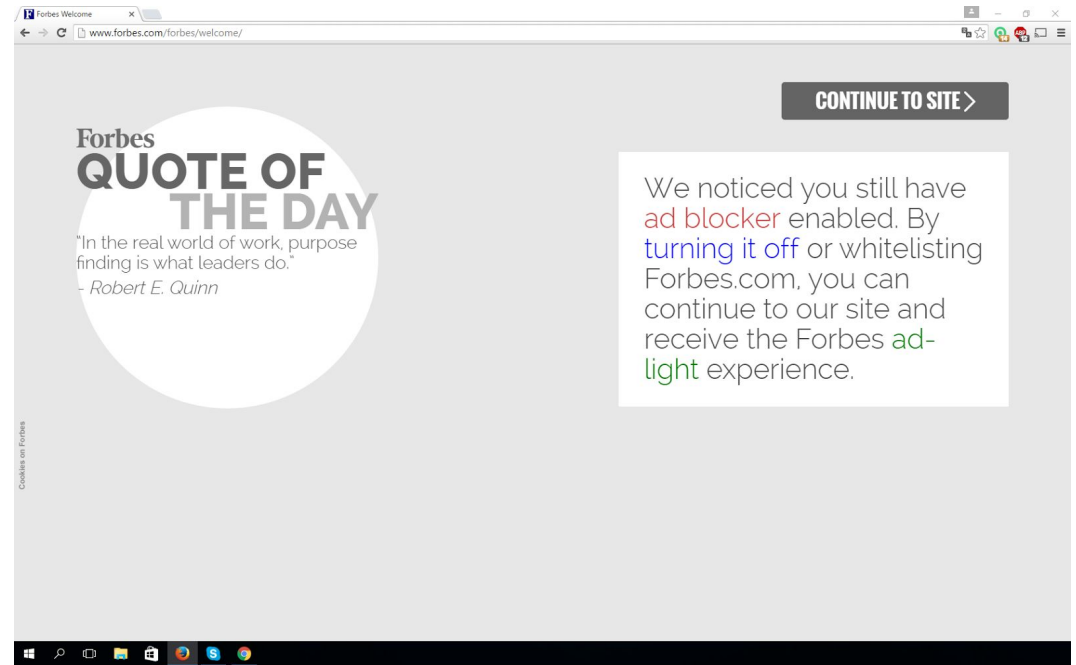


Increase User Experience

- Most popular Chrome extension
 - > 40,000,000 users
- Blocks annoying ads
- Goals clash!
 - Webpage wants to detect
 - Extension wants to remain hidden



AdBlock



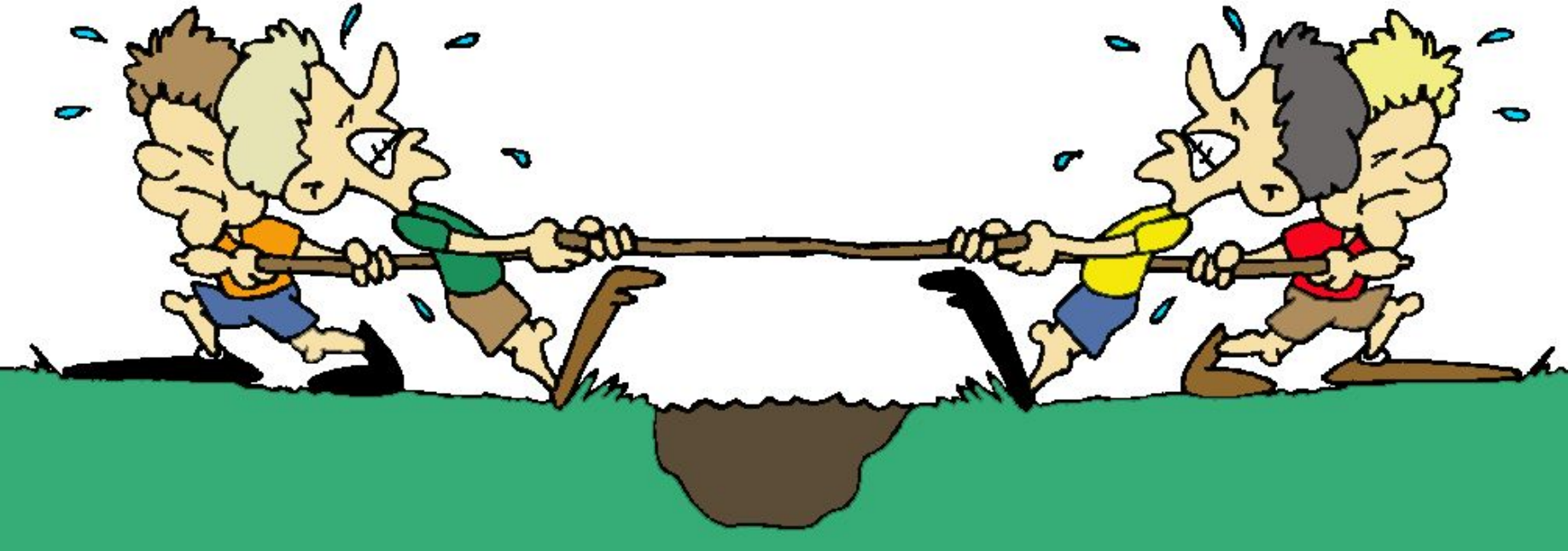
Sensitive extensions

- Password manager
 - ~4,000,000 users
- Phishing attacks
 - LostPass [1]
- Need to protect sensitive extensions!
- Detection unwanted: websites have no business detecting extensions

[1] Sean Cassidy : LostPass
<https://www.seancassidy.me/lostpass.html>



Security goals at clash



State of the art - arms race

Personal Open source Business Explore Pricing Blog Support This repository Search Sign in Sign up

sitexw / FuckAdBlock Watch 67 Star 922 Fork 118

Code Issues 13 Pull requests 0 Pulse Graphs

Detects ad blockers (Adblock, ...) <http://fuckadblock.sitexw.fr>

58 commits 4 branches 9 releases 6 contributors

Branch: master New pull request Find file Clone or download

sitexw	Clean syntax and update version	Latest commit da20a52 on 4 Mar
.gitattributes	Ignore test.html file in language statistics	9 months ago
LICENSE	Update the license and version	a year ago
README.md	Clean syntax and update version	3 months ago
bower.json	Clean syntax and update version	3 months ago
fuckadblock.js	Clean syntax and update version	3 months ago
package.json	Clean syntax and update version	3 months ago
test.html	Clean syntax and update version	3 months ago

README.md

FuckAdBlock (v3.2.1)

You can detect nasty ad blockers. Online example: <http://sitexw.fr/fuckadblock/>


State of the art - arms race

The screenshot shows the GitHub interface for the repository 'Mechazawa / FuckFuckAdblock'. At the top, there are navigation links for 'Personal', 'Open source', 'Business', 'Explore', 'Pricing', 'Blog', and 'Support'. A search bar is present with the text 'This repository' and a search button. A 'Sign in' button is also visible. Below the navigation, the repository name 'Mechazawa / FuckFuckAdblock' is displayed, along with 'Watch' (39), 'Star' (1,040), and 'Fork' buttons. A secondary navigation bar includes 'Code', 'Issues' (5), 'Pull requests' (0), 'Pulse', and 'Graphs'. The repository description reads: 'Acts like FuckAdBlock.js but always says that no adblock was detected'. Below this, statistics show '37 commits', '1 branch', '0 releases', and '7 contributors'. A yellow bar highlights the repository's main interface, including a 'Branch: master' dropdown, a 'New pull request' button, a 'Find file' button, and a 'Clone or download' button. A recent commit by 'Mechazawa' is shown, titled 'Merge pull request #19 from WaKeMaTTa/patch-1', with the latest commit hash 'dbe9f0f' on 'a mon'. Below the commit, a list of files is shown: 'FuckFuckAdblock.user.js' (Improvements proposed by @sominlee74 #18, a mon) and 'README.md' (Simplified installation, 5 month). The 'README.md' file is selected, and its content is displayed below. The title 'FuckFuckAdblock' is prominently displayed in a large, bold font. The text below the title reads: 'A simple userscript that acts like FuckAdBlock.js (A well known adblock detector) but always says that no adblock was detected. Just install it using [Tampermonkey](#) (chrome) or [Greasemonkey](#) (Firefox) by clicking [here](#) and try it out at <http://sitexw.fr/fuckadblock/>. FuckFuckAdblock works on any version of FuckAdBlock. It's kinda like a trace buster buster'.

State of the art - arms race

GitHub Gist [All gists](#) [GitHub](#) [Sign up](#)

Instantly share code, notes, and snippets.

 [clsr](#) / **FuckFuckFuckAdBlock.js**
Last active 5 months ago

[Code](#) [Revisions 2](#) [Stars 1](#) [Embed](#) `<script src="https://gi`

Fixes FuckFuckAdBlock.user.js' modifications to window.fuckAdBlock

```
FuckFuckFuckAdBlock.js  
1  /*  
2  This software is released into public domain.  
3  It is provided "as is", without warranties or conditions of any kind.  
4  Anyone is free to use, modify, redistribute and do anything with this software.  
5  */  
6  
7  if (!(window.fuckAdBlock instanceof window.FuckAdBlock)) {  
8      var fab = new window.FuckAdBlock(window.fuckAdBlock._options);  
9      for (var field in fab) {  
10         window.fuckAdBlock[field] = fab[field];  
11     }  
12 }
```

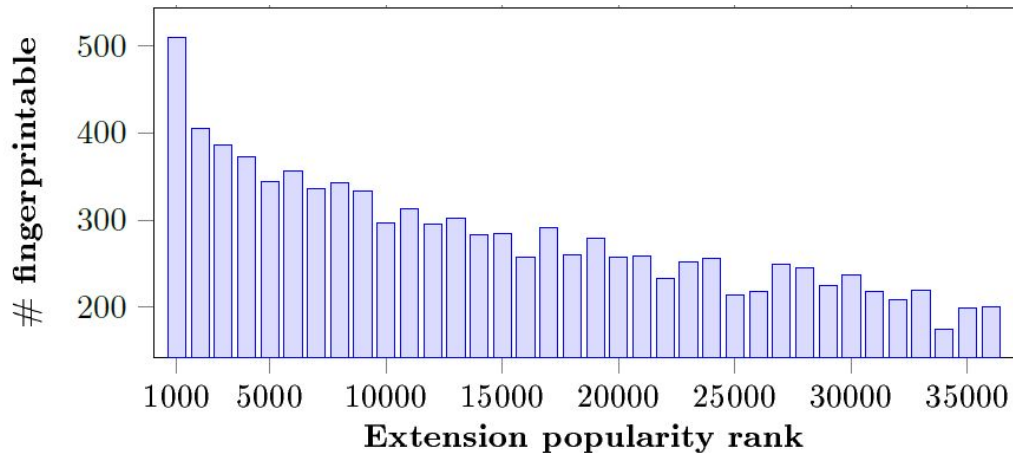
Non-behavioral fingerprinting

- Download extensions from Chrome and Mozilla extension stores
- Analyse the manifest files
 - `web_accessible_resources`
 - `contentaccessible=yes`
- Generate map based on manifest files
- PROFIT!



Empirical Study - Chrome

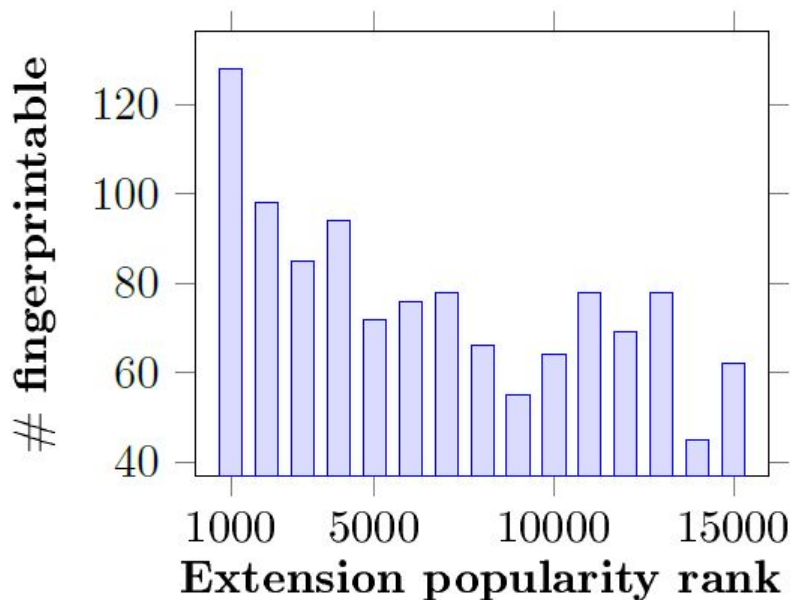
- ~36,000 extensions
- 28.1% fingerprintable
 - 80% of top 10!
 - 60% of top 100!
 - 51% of top 1000!



Extension	# of users
Adblock	10,000,000+
Avast Online Security	10,000,000+
LastPass	3,917,267
Ghostery	2,365,971
Privacy Badger	290,811

Empirical Study - Firefox

- ~15,000 extensions
- 7.68% fingerprintable
 - 12.8% of top 1000
- None of Ghostery, LastPass or AdBlock



No manifest file	6,560
Fingerprintable	1,148
No accessible resources	7,213
# of extensions	14,921

Empirical Study - Alexa top 10,000

- 12 webpages attempted to access resources
 - Only Chrome extensions were attempted
- 21 distinct extensions
 - 2 seemingly malware
- 7 extensions no longer in Chrome webstore

#	Extension ID	Extension name	in web store	Extension type
ext_A	ahkgkxhcbfalobbfmghfgcpalihbllkm	Notificador de Estrenos	-	malware(?)
ext_B	bfbmjmiodbnnpllbbbfblcplfjjepjdn	Turn Off the Lights	✓	media
ext_C	bfegaehidkkcfaikpaijcdahnpikhobf	Gismeteo	✓	weather
ext_D	bgnkhhnamicmpeenaelnjfhikgbkllg	Adguard AdBlocker	✓	adblocker
ext_E	boadgeojelhgndaghljhdicfkmllpafd	Google Cast	✓	media
ext_F	cfhdojbkjhnklbpkdaibdcdddilifddb	Adblock Plus	✓	adblocker
ext_G	dehahmmihbedjejfjcebfkihbfgkedlf	Añadir tumi Gratis	-	malware(?)
ext_H	dliochdbjfkdbacpmhlcpmlaejidimm	Google Cast (Beta)	✓	media
ext_I	enhhojjnijigcajfpahajepfemndkmdlo	Google Cast (old)	-	media
ext_J	eobejphpabbjeehffmbieckpkggpbai	네이버 톨바	✓	productivity
ext_K	epcnfbjfcgphgdmggkamkgojdagdnn	uBlock	✓	adblocker
ext_L	fmfcbgogabcblcofgocippekhfcmgfj	Google Cast (old)	-	media
ext_M	fndlhnahedoklpdaacidomdnplcjcpj	Adblock Premium	-	adblocker
ext_N	gighmmpiobklfepjocnamgkkbiglidom	Adblock	✓	adblocker
ext_O	hfaagokkkhdbgiakmmlclaapfelngoah	Google Cast (old)	-	media
ext_P	kloiceblkiijklknknaibcaieicafajlo	RT News	✓	news
ext_Q	knebihmckndhiglamoabbnifdkijidd	Adblock Super	-	adblocker
ext_R	mcefmojpphnceadnghednjhbmphipkb	AdRemover	✓	adblocker
ext_S	mlomiejdfoiklichcflejclcbmpeanii	Ghostery	✓	privacy
ext_T	ocifcklkibdehekfnmflempfgjhbedch	Adblock Pro	✓	adblocker
ext_U	phoocsmelibnehglfgjfhogfohjmgllgh	Новости дня СМИ2	✓	news

Empirical Study - Alexa top 10,000

Rank	Domain	Extension	XHR					GET						
			C	F	S	O	M	E	C	F	S	O	M	E
127	twitch.tv	ext_E, ext_H, ext_I, ext_L, ext_O	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-
478	rt.com	ext_P	✓	-	-	-	-	✓	-	-	-	-	-	-
564	gismeteo.ru	ext_C	-	-	-	-	-	-	✓	-	-	-	-	✓
1678	smi2.ru	ext_U	✓	-	-	-	-	✓	-	-	-	-	-	-
1917	pelis24.com	ext_G	-	-	-	-	-	-	✓	-	✓	-	-	-
2012	popmyads.com	ext_S	-	-	-	-	-	-	✓	-	-	-	-	✓
2486	what-character-are-you.com	ext_N	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
4083	netvibes.com	ext_D, ext_F, ext_K, ext_M, ext_N, ext_Q, ext_R, ext_T	✓	-	-	-	-	-	-	-	-	-	-	-
4369	mt.co.kr	ext_J	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
5507	yaske.cc	ext_A	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
6486	stc.com.sa	ext_B	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
9553	pikolive.com	ext_E, ext_H, ext_I, ext_L, ext_O	✓	-	-	-	✓	✓	-	-	-	-	-	-

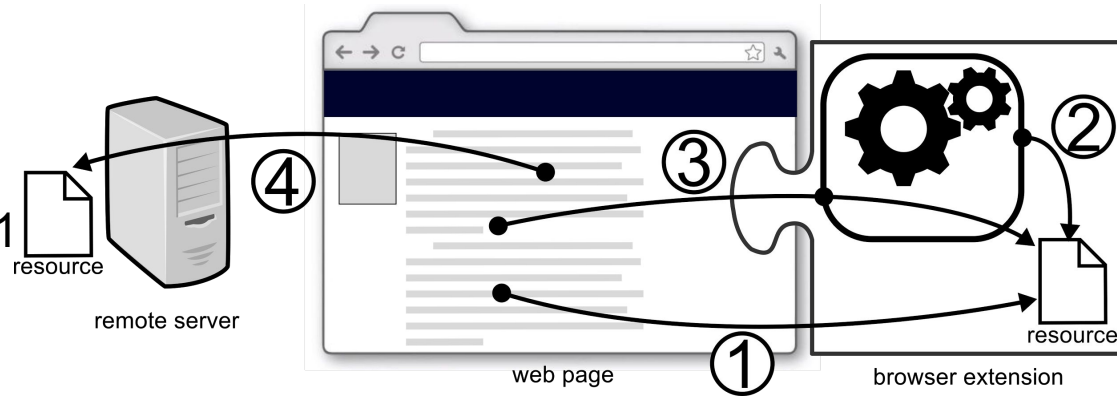
Measures - Web pages

- Web pages whitelist extensions
 - Proposes who is allowed to execute in their domain
- Extensions can be temporarily enabled/disabled, depending on whitelist



Measures - Extensions

- No direct access from webpage to extension (#1)
 - Use message passing (#3)
- Fetch resources from server (#4)
 - Caching problems
 - Privacy concerns
- Tracking script provenance
 - Distinguish between different #1
- Use data URIs
- Randomize extension IDs
- Whitelist of webpages
 - Allow #1 if webpage is trusted
 - No need to enable e.g. Google Cast on non-streaming sites



Whitelist arbitration



- users > developers > browser
 - Practiced by Google
- User arbiter to resolve the conflict
 - Temporarily enable/disable extension depending on webpage
 - Override the whitelist

Thank you!

Questions?

(Try demo at: <https://goo.gl/xfeiPj>)