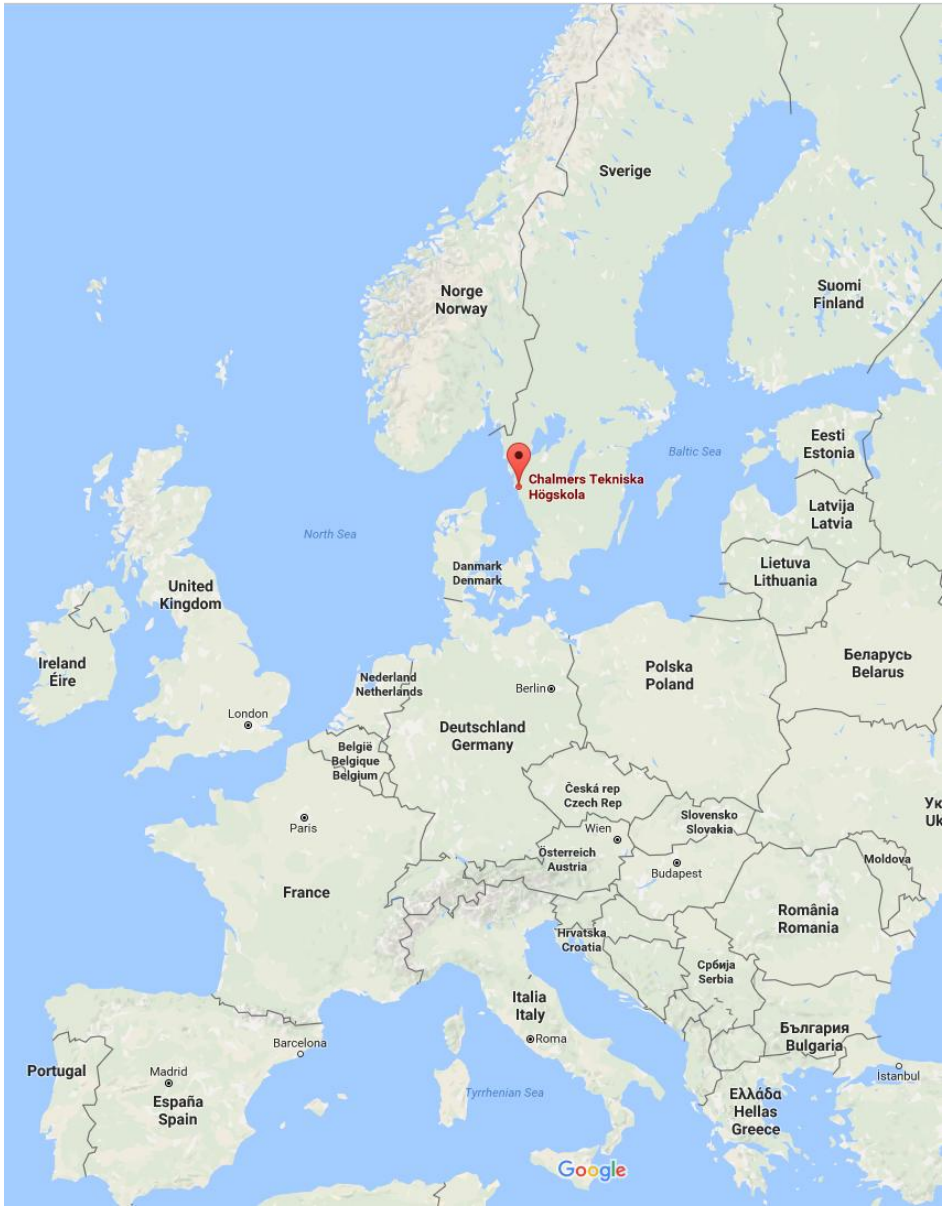
Chalmers University of Technology



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
- **<u>Enrich functionality and user experience!</u>**

Goals of websites

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

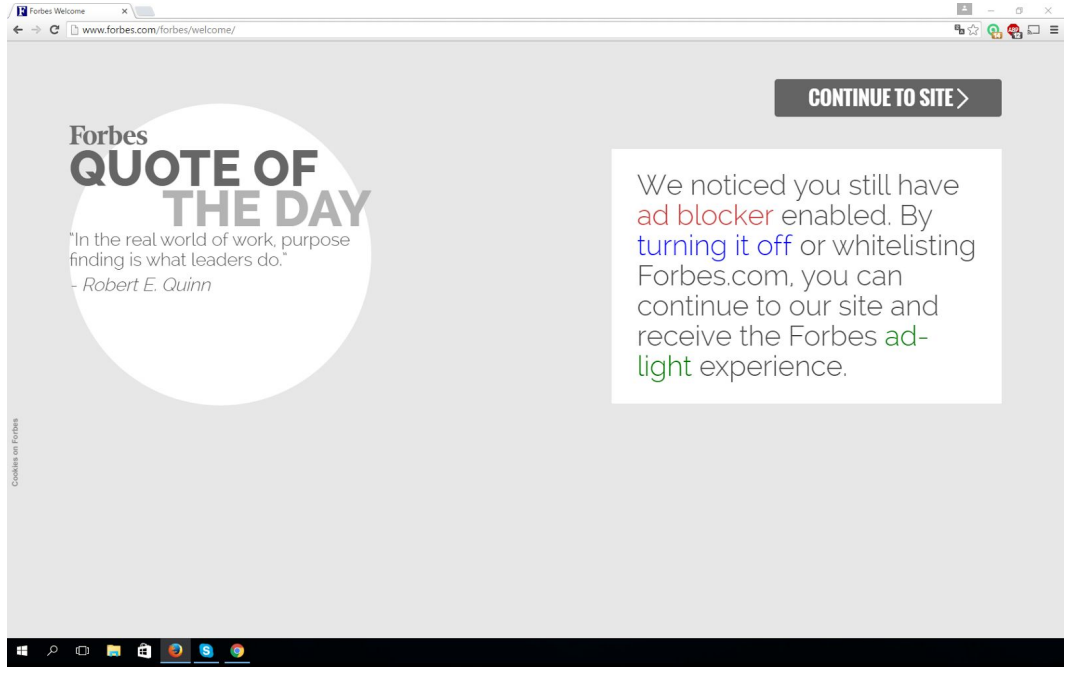
Goals of websites

- 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

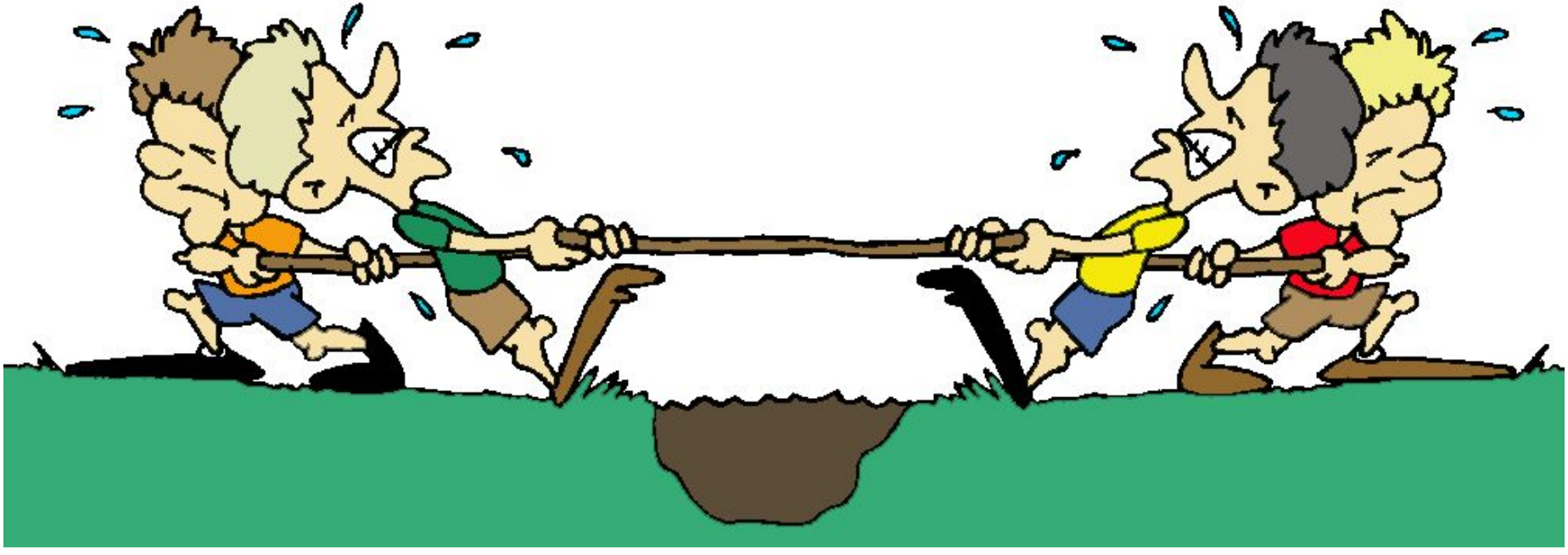


Sensitive extensions

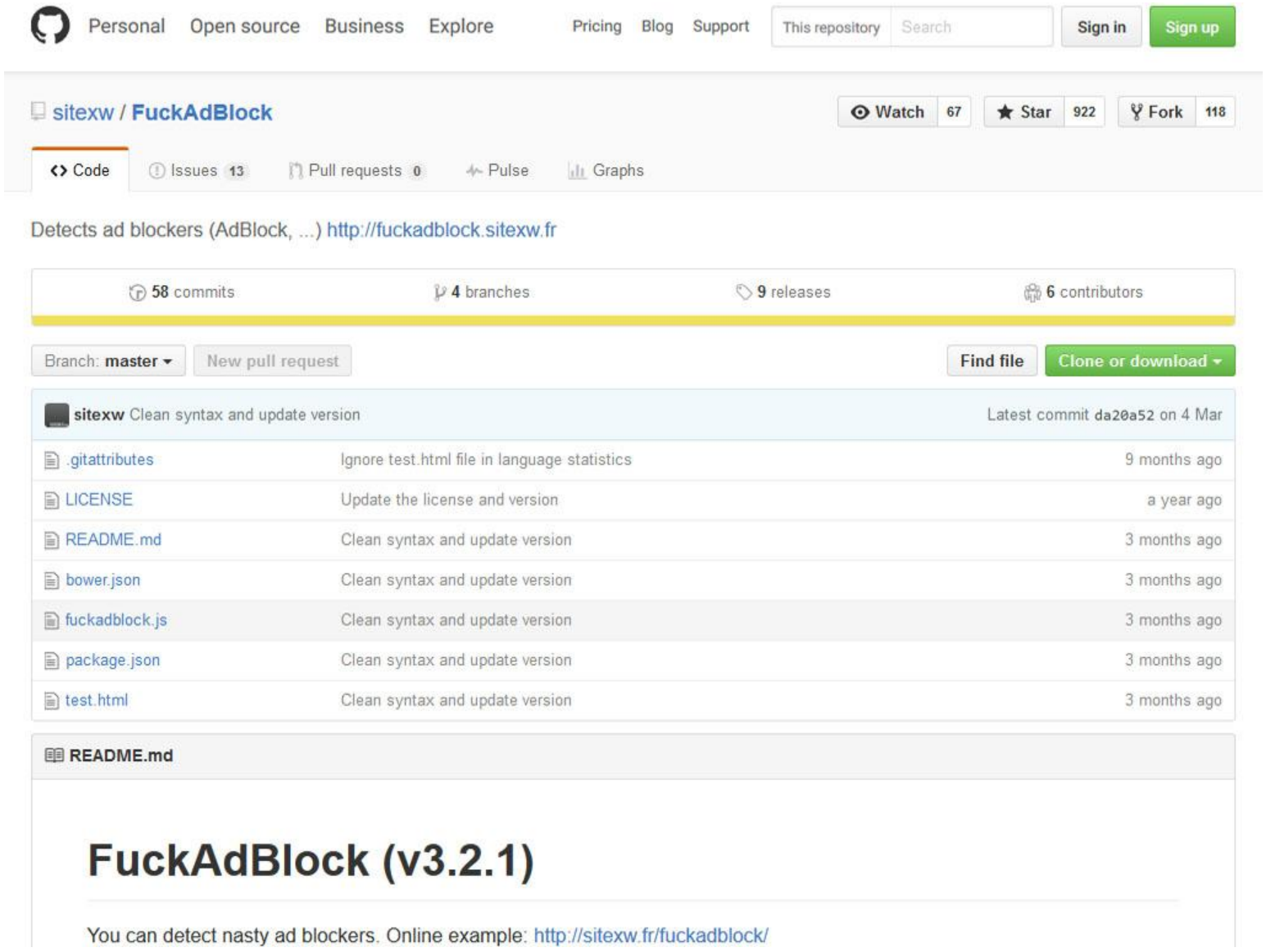
- Password manager
  - ~4,000,000 users
- Phishing attacks
  - LostPass [1]
- Need to protect sensitive extensions!
- Detection unwanted: websites have no business detecting extensions

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

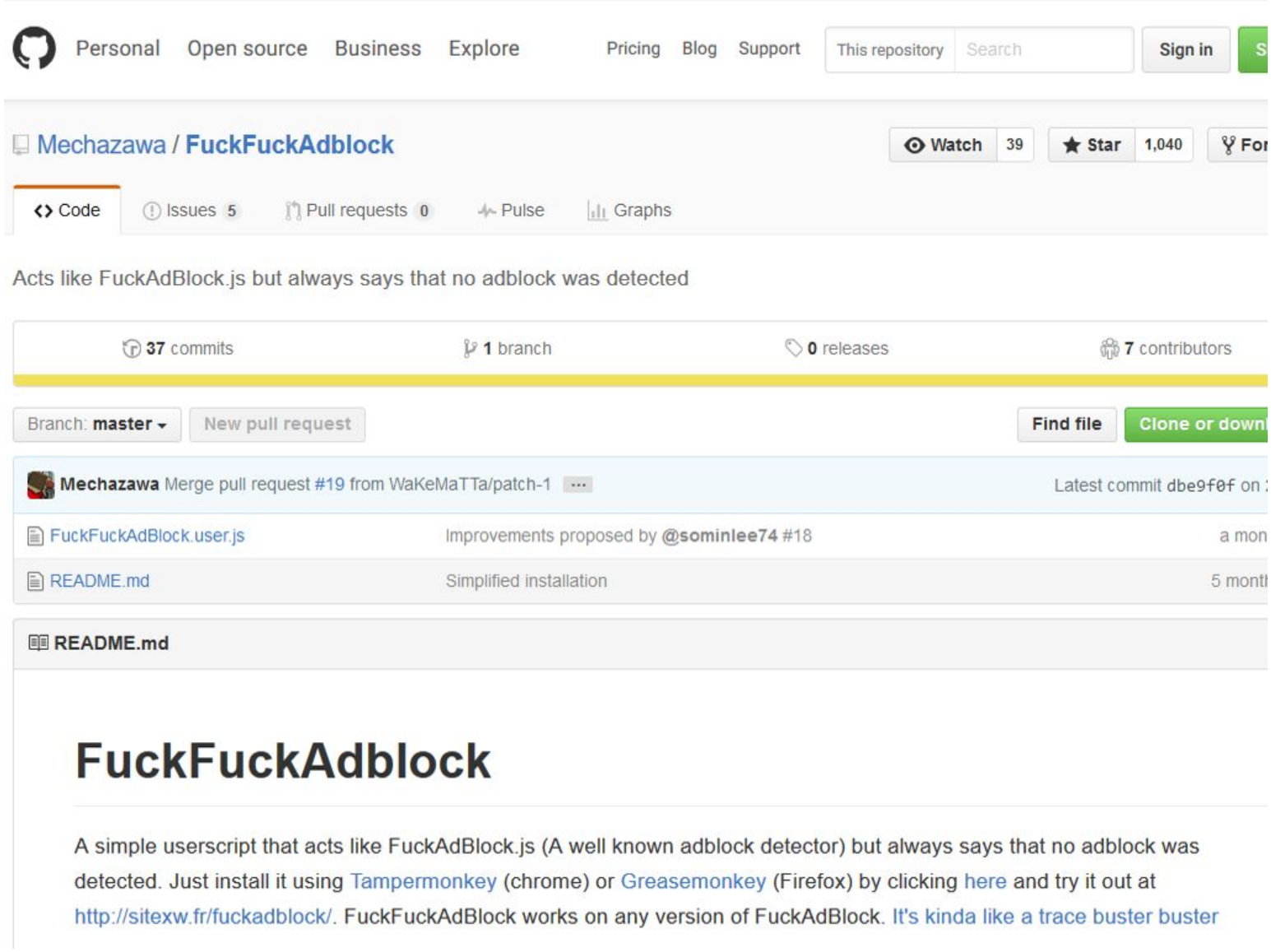
Security goals at clash



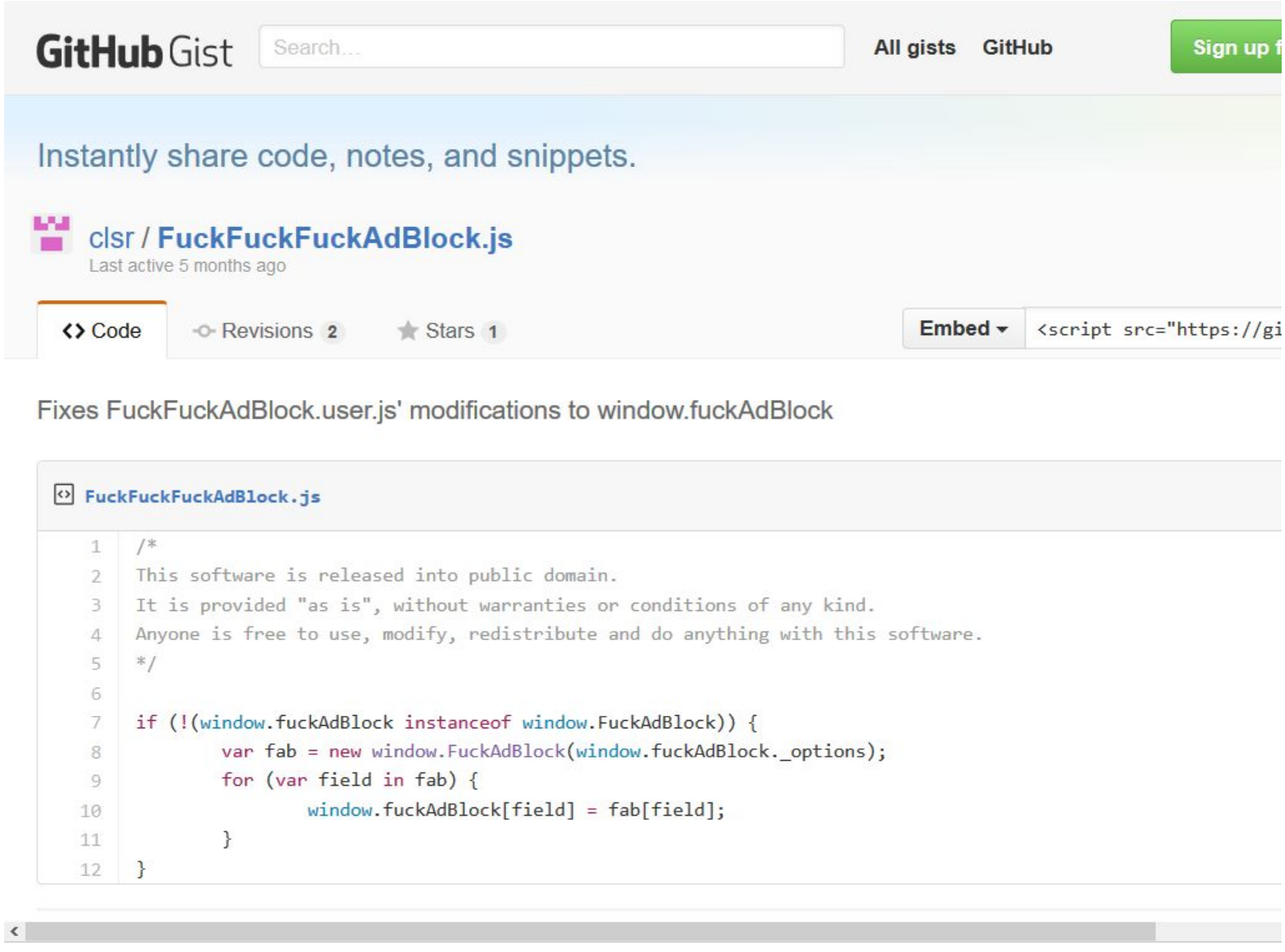
State of the art - arms race



State of the art - arms race



State of the art - arms race

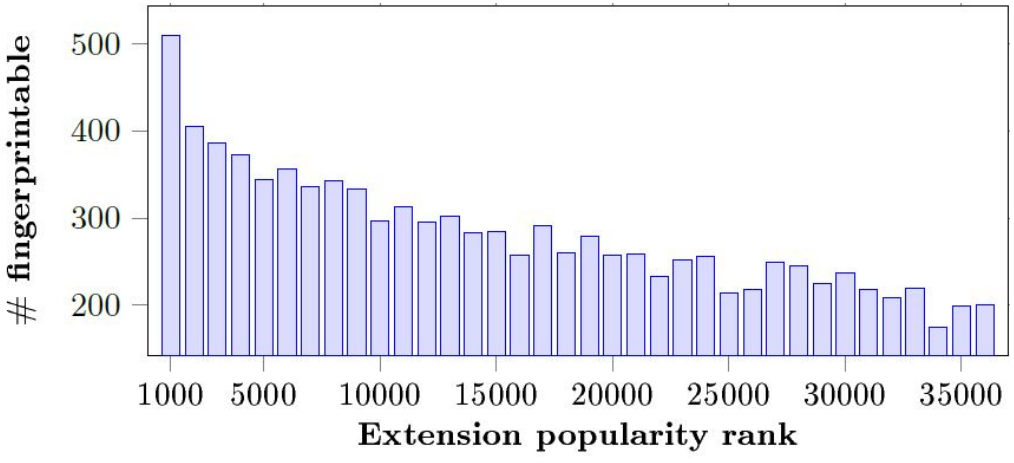


Non-behavioral fingerprinting

- 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

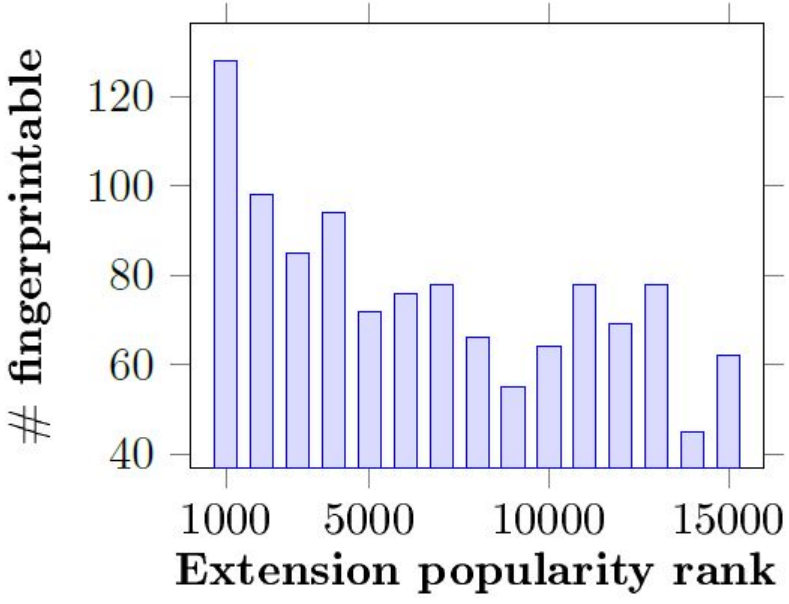
- ~36,000 extensions
- 28.1% fingerprintable
  - 80% of top 10!
  - 60% of top 100!
  - 51% of top 1000!



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	ahkgkkhcbfalobbfmhgfgcpalihbllkm	Notificador de Estrenos	–	malware(?)
ext_B	bfbmjmiodbnnpllbbbfblcplfjjepjdn	Turn Off the Lights	✓	media
ext_C	bfegaehidkkcfaikpaijcdahnpikhobf	Gismeteo	✓	weather
ext_D	bgnkhhnnamicmpeenaelnjfhikgbkllg	Adguard AdBlocker	✓	adblocker
ext_E	boadgeojelhgndaghljhdicfkmllpafd	Google Cast	✓	media
ext_F	cfhdojbkjhnklbpkdaibdccddilifddb	Adblock Plus	✓	adblocker
ext_G	dehahmmihbedjejfjcebfkihbgfkedlf	Añadir tumi Gratis	–	malware(?)
ext_H	dliochdbjfkdbacpmhlcpmleaejidimm	Google Cast (Beta)	✓	media
ext_I	enhhojjnijigcajfphajepfemndkmdlo	Google Cast (old)	–	media
ext_J	eobejphpabbjeehffmbiecckpkggpbai	네이버 툴바	✓	productivity
ext_K	epcnnfbjfcgphgdmggkamkmgojdagdnn	uBlock	✓	adblocker
ext_L	fmfcbgogabcbclcofgocippekhfcmgfj	Google Cast (old)	–	media
ext_M	fndlhnanhedoklpdaacidomdnplcjcpj	Adblock Premium	–	adblocker
ext_N	gighmmpiobklfepjocnamgkkbiglidom	Adblock	✓	adblocker
ext_O	hfaagokkkhdbgiakmmlclaapfelnkoah	Google Cast (old)	–	media
ext_P	kloiceblkijlknknaibcaieiicafajlo	RT News	✓	news
ext_Q	knebimhcckndhiglamoabbnifdkijidd	Adblock Super	–	adblocker
ext_R	mcefmojpghnaceadnghednjhbmphipkb	AdRemover	✓	adblocker
ext_S	mlomiejdfkolichcflejclcbmpeaniij	Ghostery	✓	privacy
ext_T	ocifcklkibdehekfnmflempfgjhbedch	Adblock Pro	✓	adblocker
ext_U	phoocmemlibnehglfgjfhogfohjmglgh	Новости дня СМИ2	✓	news

Empirical Study - Alexa top 10,000

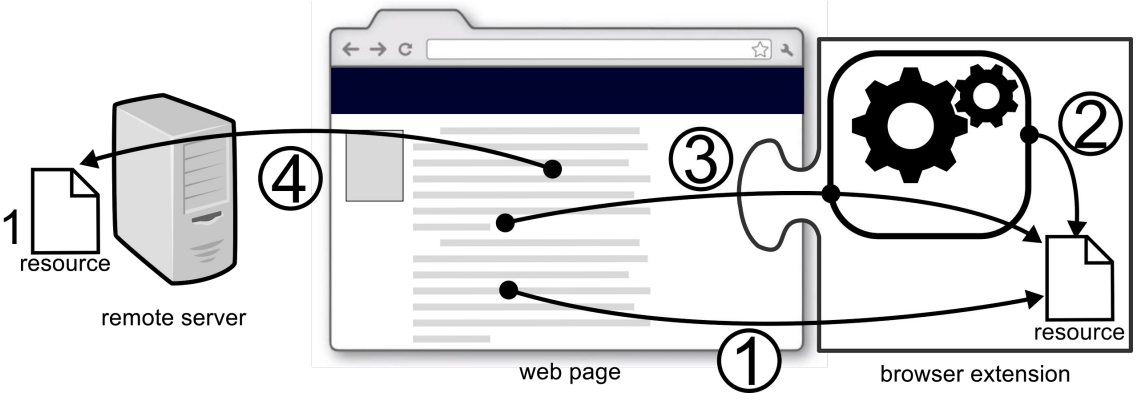
Rank	Domain	Extension	XHR						GET					
			C	F	S	O	M	E	C	F	S	O	M	E
127	twitch.tv	ext_E, ext_H, ext_I, ext_L, ext_O	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
478	rt.com	ext_P	✓	–	–	–	–	✓	–	–	–	–	–	–
564	gismeteo.ru	ext_C	–	–	–	–	–	–	✓	–	–	–	–	✓
1678	smi2.ru	ext_U	✓	–	–	–	–	✓	–	–	–	–	–	–
1917	pelis24.com	ext_G	–	–	–	–	–	–	✓	–	✓	–	–	–
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)