GÉANT
Networks • Services • People

Browser Security and Privacy

Leaving fewer traces and improving web client security

Klaus Möller
WP8-T1

Webinar, 21st of September 2020

Public

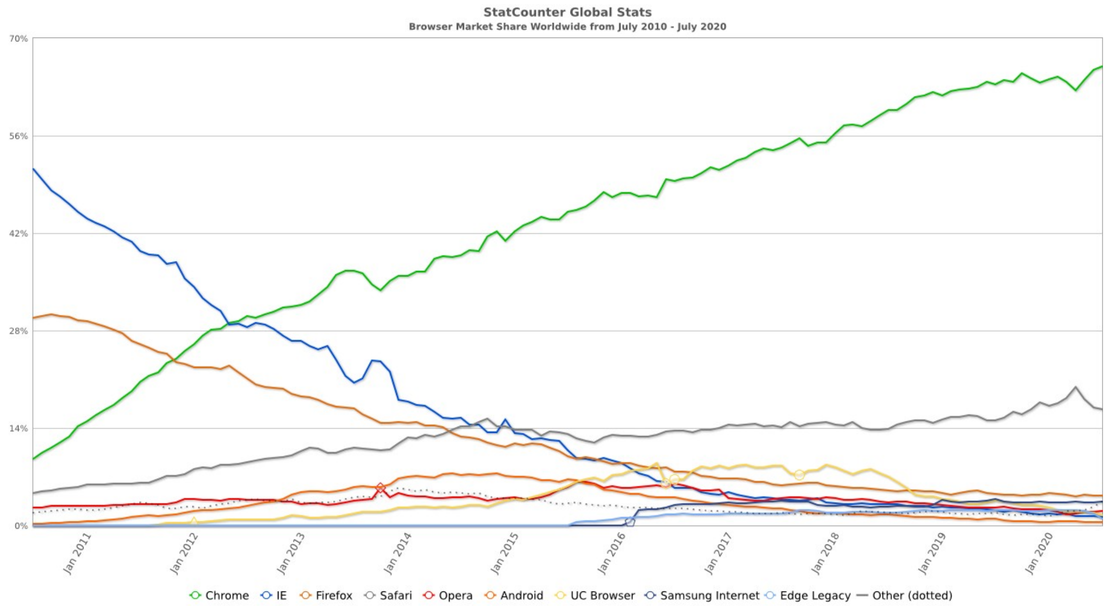
www.geant.org

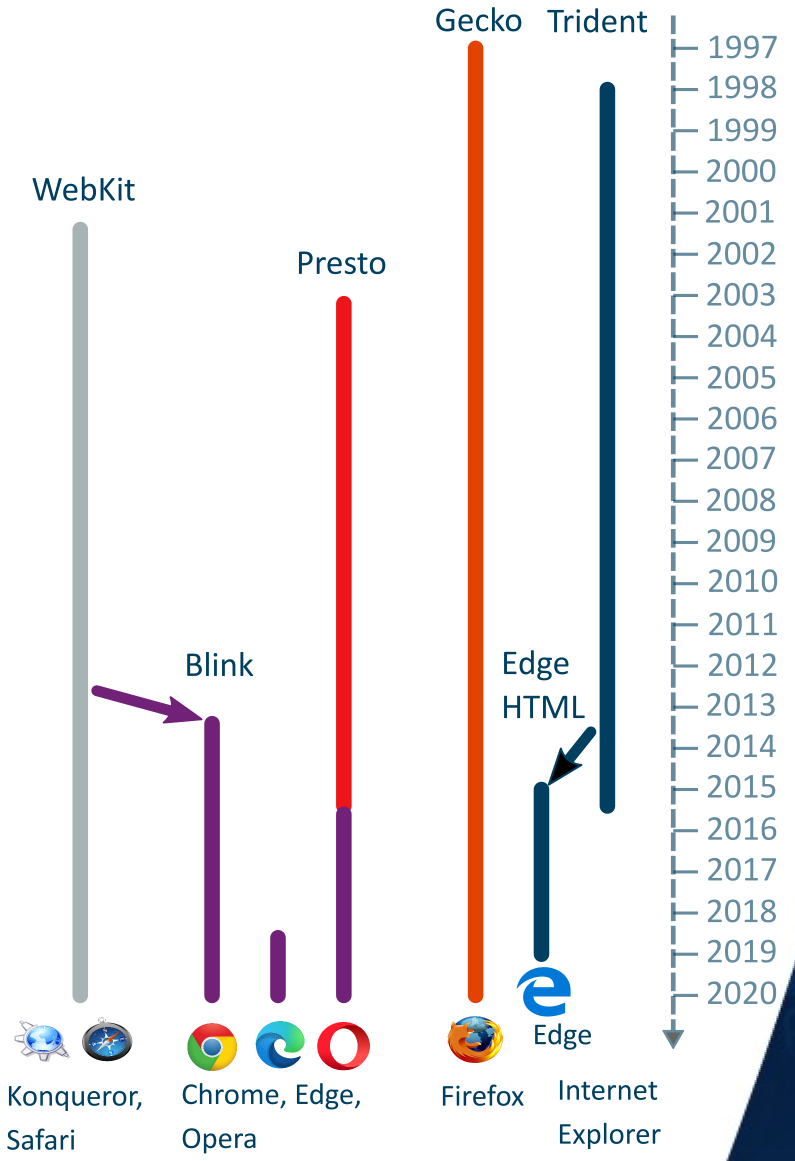
Web Browsers

- **The** universal client today
  - For all kinds of web-based applications
  - Additionally: Custom Apps that are browsers in disguise (i.e. build around browser engine)
- One client for **all** kinds of applications
  - From leisure to sensitive/financial/personal information
  - The best point of attack as the victim comes to the attacker
- Firewalls/Anti-Virus of limited effectiveness
  - Malware download through Outgoing HTTP(S) connection – almost always allowed and often not scanned by proxies
  - Anti-Virus often evaded/don't recognize new malware

Web Browser Engines

- The core logic of the web browser
  - Blink & Gecko practically own the market
  - Except WebKit on iOS (only engine allowed there)
  - Forked engines often share vulnerabilities




WebKit

Presto

Gecko

Trident

Blink

Edge HTML

Konqueror, Safari

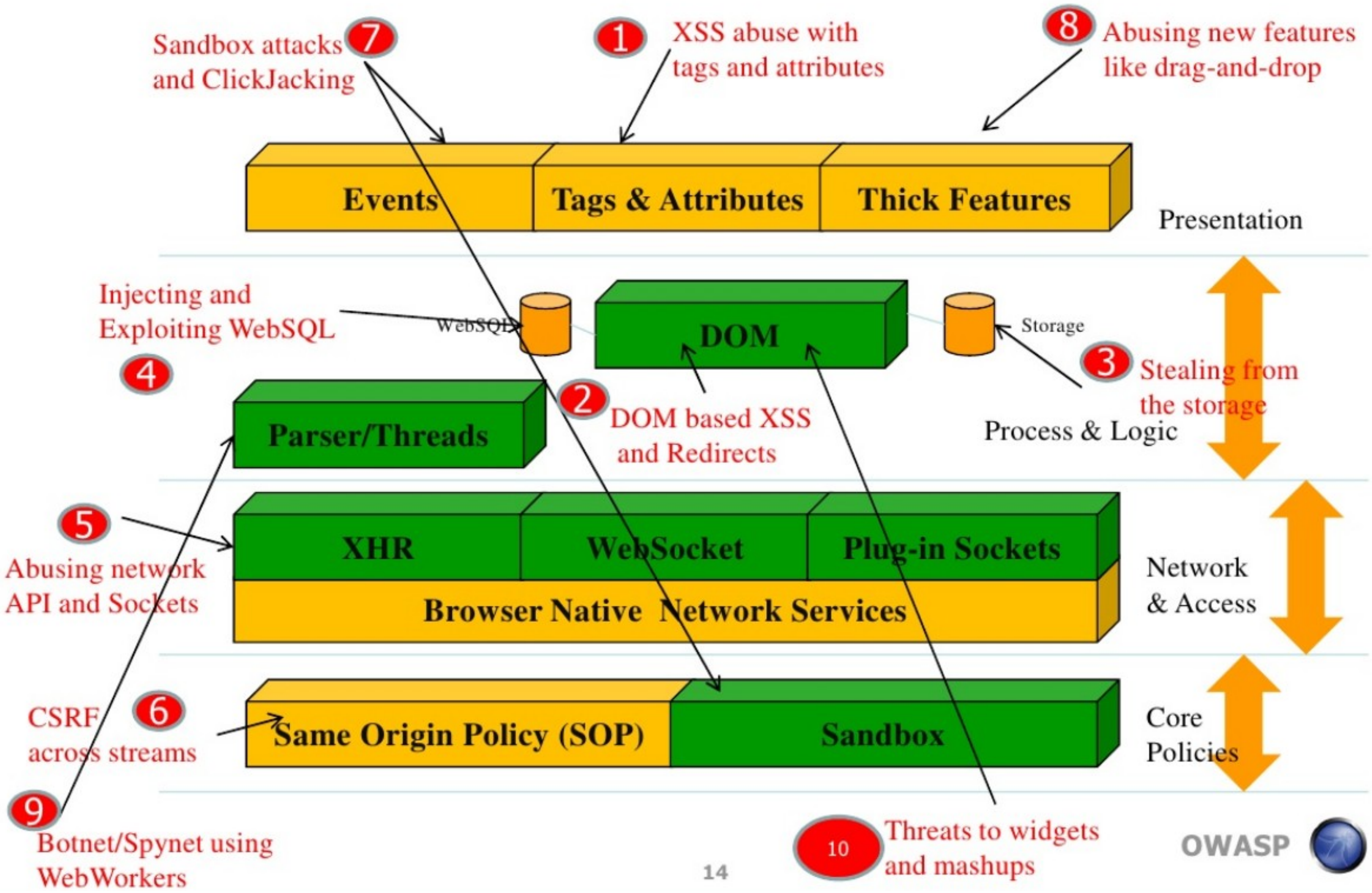
Chrome, Edge, Opera

Firefox

Edge

Internet Explorer

Web Browser Threat Model



7 Sandbox attacks and ClickJacking
1 XSS abuse with tags and attributes
8 Abusing new features like drag-and-drop
Events
Tags & Attributes
Thick Features
Presentation
Injecting and Exploiting WebSQL
4
WebSQL
DOM
Storage
3 Stealing from the storage
2 DOM based XSS and Redirects
Parser/Threads
Process & Logic
5 Abusing network API and Sockets
XHR
WebSocket
Plug-in Sockets
Browser Native Network Services
Network & Access
CSRF across streams
6
Same Origin Policy (SOP)
Sandbox
Core Policies
9 Botnet/Spynet using WebWorkers
14
10 Threats to widgets and mashups
OWASP

Browser attack vectors

- The browser itself: XSS, CSRF, Clickjacking, …
- Its helper programs: Flash, PDF reader, Office suites, Java, …
- Indirectly through programs that use the browser engine
- URL-aware programs that open browsers (when clicking on the URL)

Security Problem #1: JavaScript

- Alias ECMA Script, ActionScript (Adobe), etc.
  - Basis for practically every web-application today
  - Not limited to web-browsers: PDF-Reader, Flash-Player, or stand-alone (Node.js)
- JavaScript Code is “limited” (cf. sandbox)
  - No direct access to files, camera, microphone, etc. except through browser
  - No access to content and code from other domains/sites (same origin policy)
- Additional problem, esp. for Firefox
  - Browser Functions and GUI can be accessed as DOM-objects
  - DOM code is privileged, i.e. it runs outside the sandbox
  - Needed for add-ons
- Theoretically: no security problem (if implemented properly)

Dealing with JavaScript: Patching

- In practice: an endless number of exceptions and implementation mistakes
  - Esp. with regards to separation of DOM/non-DOM contexts

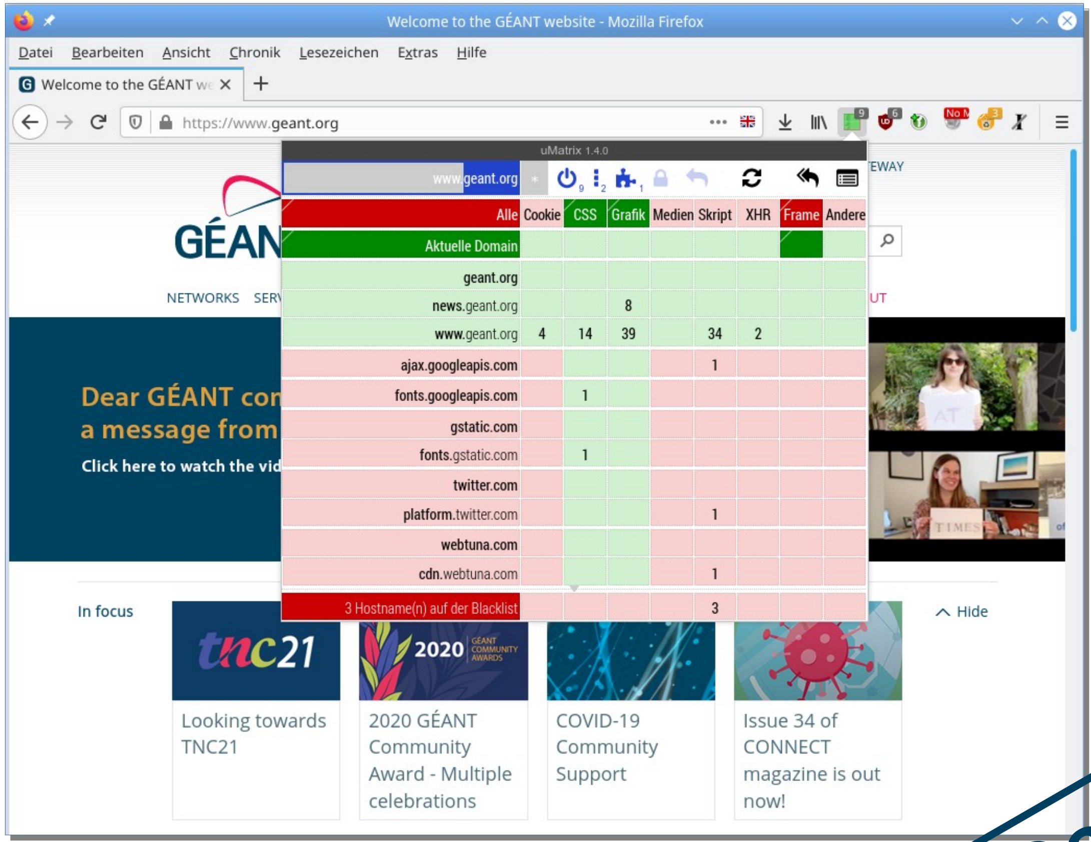
→ Every month a new round of patches

- Auto Update: Recommended for self-administered browsers
  - Don’t forget the installations on USB-drives
  - Turn off if you don’t have the rights to write to the installation directories
- Extended Service Release (ESR) or Long Term Support (LTS):
  - Backporting of security patches by browser vendor
  - Updates often through OS (Linux) distribution vendor
  - Recommended for managed environments
  - A bit more control over when to patch/update

Dealing with JavaScript: Restricting

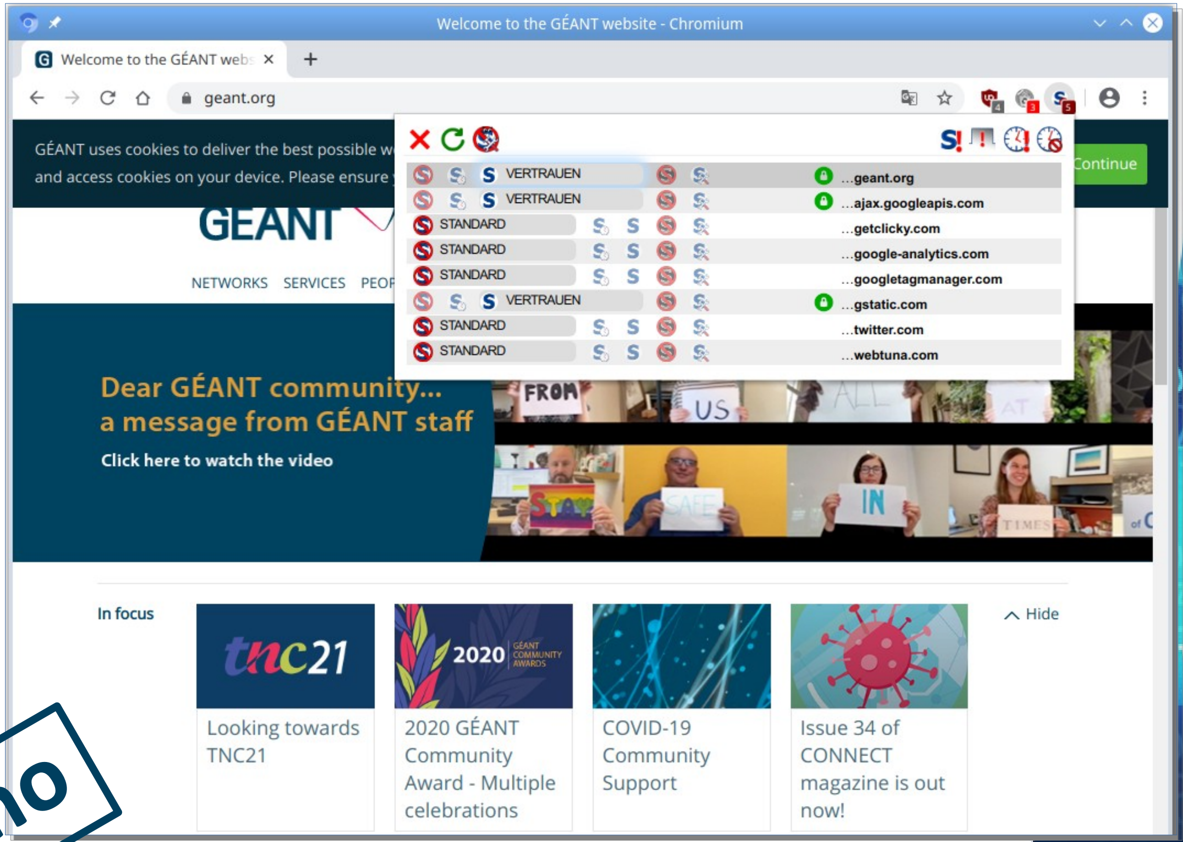
- Turning JavaScript off in general
  - Not feasible – Too much functionality depends on JavaScript today
- Restrict JavaScript to specific sites is possible
  - Especially third-party sites
- Add-ons
  - NoScript: Firefox, Chrom*
  - uMatrix: Firefox, Chrom*
    - Still in app stores but development put on hold, Sept. 18th, 2020

JavaScript Live Demonstration: NoScript & uMatrix


Welcome to the GÉANT website - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Welcome to the GÉANT we
https://www.geant.org
uMatrix 1.4.0
www.geant.org
GÉAN
NETWORKS SER
Dear GÉANT con
a message from
Click here to watch the vid
In focus
Hide

Alle	Cookie	CSS	Grafik	Medien	Skript	XHR	Frame	Andere
Aktuelle Domain								
geant.org								
news.geant.org			8					
www.geant.org	4	14	39		34	2		
ajax.googleapis.com					1			
fonts.googleapis.com		1						
gstatic.com								
fonts.gstatic.com		1						
twitter.com								
platform.twitter.com					1			
webtuna.com								
cdn.webtuna.com					1			
3 Hostname(n) auf der Blacklist					3			

tnc21
Looking towards TNC21
2020 GÉANT Community Awards
2020 GÉANT Community Award - Multiple celebrations
COVID-19 Community Support
Issue 34 of CONNECT magazine is out now!


Welcome to the GÉANT website - Chromium
Welcome to the GÉANT webs
geant.org
GÉANT uses cookies to deliver the best possible w
and access cookies on your device. Please ensure
Continue
GÉANT
NETWORKS SERVICES PEOP

VERTRAUEN	...geant.org
VERTRAUEN	...ajax.googleapis.com
STANDARD	...getclicky.com
STANDARD	...google-analytics.com
STANDARD	...googletagmanager.com
VERTRAUEN	...gstatic.com
STANDARD	...twitter.com
STANDARD	...webtuna.com

Dear GÉANT community...
a message from GÉANT staff

Click here to watch the video

FROM
US
ALL
AT
STAY
SAFE
IN
TIMES
In focus
Hide
tnc21
2020 GÉANT Community Awards

- Looking towards TNC21
- 2020 GÉANT Community Award - Multiple celebrations
- COVID-19 Community Support
- Issue 34 of CONNECT magazine is out now!

Demo

JavaScript Restricting Add-ons

- Basic Principle: Select what kind of content is allowed from what sites
- Sites: Identified by host/domain name
  - Most specific match (i.e. longest suffix)
- Content type: JavaScript, XHR, Frames, Cookies
  - Set of content types differs between Add-ons
- In practice: It takes some time to configure sites to run error-free
  - Several reloads necessary for new sites

JavaScript Add-ons in Practice

- Pros:
  - Prevents malware downloads in drive-by infections effectively
  - Also prevents most advertisment loading and tracking
- Cons:
  - Kills useful third party content: Captchas, federated logins, etc.
    - Need to whitelist or enable for each site
  - Every new site visited takes time to configure – i.e. several reloads
    - Re-entering form data may be annoying
  - Even known sites require work after site changes – constant work

Security Problem #2: Plug-ins

- Plug-ins extend browser capabilities to display content
  - Other formats, e.g. PDF, VRML, Office,
  - Interpreter for programming languages: Java, PHP, Python, …
  - Mixed formats: Flash, Silverlight
- Interface
  - Old: NAPI (Firefox <=56), Active-X, Browser Helper Objects (Internet Explorer)
  - Today: Web-Extensions (Firefox >= 57, Chrom*)

Plugins from the Attackers Perspective

- Often the same Plugin even for different browsers
  - Means the same exploit for a plug-in will work with different browsers
- Plugins usually not sandboxed
- May be executed in the browsers address space
  - So the plug-in can access data in the browser directly
  - This includes data that will be encrypted in transport (HTTPS)
- Some plugins have their own JavaScript interpreter (e.g. Adobe)
- Complex formats → many implementation errors
- → many vulnerabilties/avenues of attack

Plugins: Mitigation

- Use separate browsers (or profiles/containers) for different activities
- Remove unused add-ons/extensions/plugins
- Flash, Silverlight, Java: Uninstall
  - If really needed, keep and disable, enable only for necessary sites
  - Java Sandbox is riddled with holes that allow break-outs
  - Alternative JVM, Flash-Player
    - Either (IBM) shares too much code … and vulnerabilties
    - Or is unstable or has too many limitations for practical use
- PDF: Alternative viewer without JavaScript support
  - JavaScript is usually not needed in PDFs
  - But almost always used by JS exploits
  - PDF Forms do not need JavaScript
  - For example: Sumatra PDF (Windows), Okular/Evince (KDE/Gnome)

Transport Encryption

- TLS (formerly SSL): The S in HTTPS
  - Protocol layer between HTTP and TCP (layer 4.5 so to speak)
  - Key management is done with X.509 certificates
  - “Three gurantees”: server authentication, data integrity, data confidentiality
  - Optionally: Client authentication
- Recommendation: Use TLS whenever possible
  - Use ***HTTPS everywhere*** add-on to force use of TLS when site uses plain HTTP and HTTPS
  - Sites should use HTTP Strict Transport Security (HSTS) HTTP Header if using both HTTP and HTTPS

Configuring Transport Encryption

- Use most recent TLS version (i.e. 1.3):
  - Use TLS 1.2 only if you have to (i.e. site doesn’t support TLS 1.3)
  - SSLv2, SSLv3, TLS 1.0, and TLS 1.1 no longer supported by browsers
  - See `security.tls.*` in `about:config` (Firefox)
  - See `SSLVersionMin` object in Group Policy (Windows Edge)
- Use secure cipher suites, i.e. those with high key lenghts
  - RSA, DH ≥ 3072, EC ≥ 512, AES ≥ 256, etc.
  - See ENISA Algorithms, key size and parameters report 2014
  - Don’t use broken algorithms, like MD5, SHA1, or RC4
  - See `security.ssl.*` in `about:config` (Firefox)

Any questions so far?

Next Topic: Tracking & Privacy

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

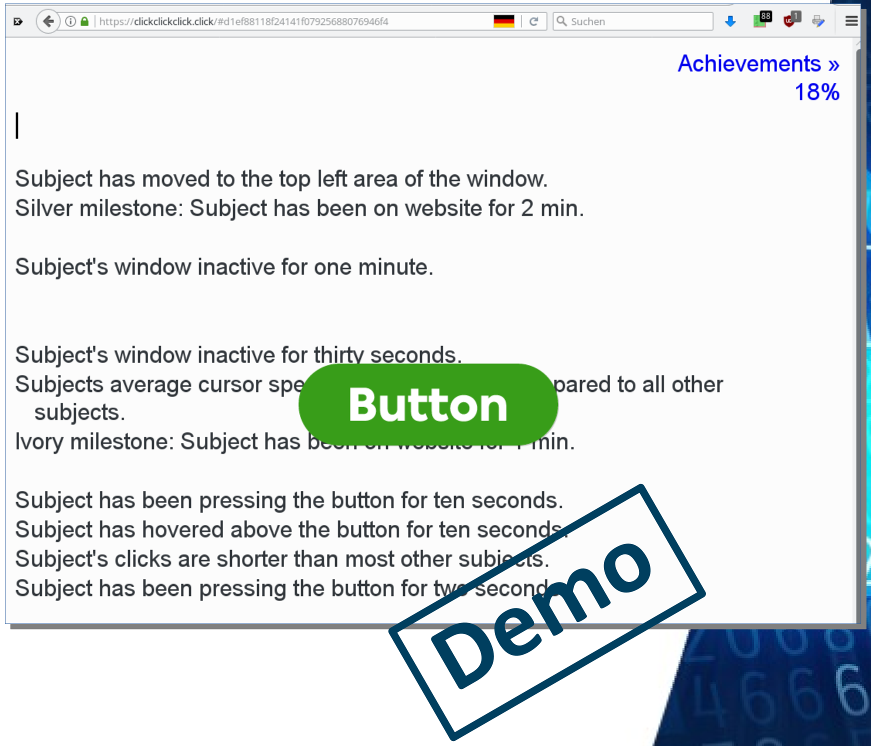
Why Tracking?

- Website owner is interested in statistical analysis of users behaviour
  - Improvements of site layout, handling, etc.
  - Advertisments for revenue
- Advertising usually supplied by third parties (advertising networks)
  - Intermediary between site owners and advertising companies
  - Targeted advertising yields more revenue
  - Thus: compile a most comprehensible user profile
- Combination of data from diverse sources
  - Cookies, browser fingerprints, web-beacons, log-in data, etc.
- The tracking of data from multiple sites makes this dangerous

What is recorded?

- Everything you do on a website is recorded and analyzed
  - How long you’ve been on a page
    - Where exactly on a page you’ve been for how long
  - From where you are coming
    - IP-address, Geolocation,HTTP Referrer, etc.
  - What you are typing
    - and whether a human is typing
  - Where/what you are clicking on
  - Asf.
- But you are rarely being informed about this fact
  - And if, the information is often vague, incomplete or misleading

https://clickclickclick.click/


https://clickclickclick.click/#d1ef88118f24141f079256880769464f4
Suchen
Achievements »
18%
Button
Demo

Subject has moved to the top left area of the window.
Silver milestone: Subject has been on website for 2 min.

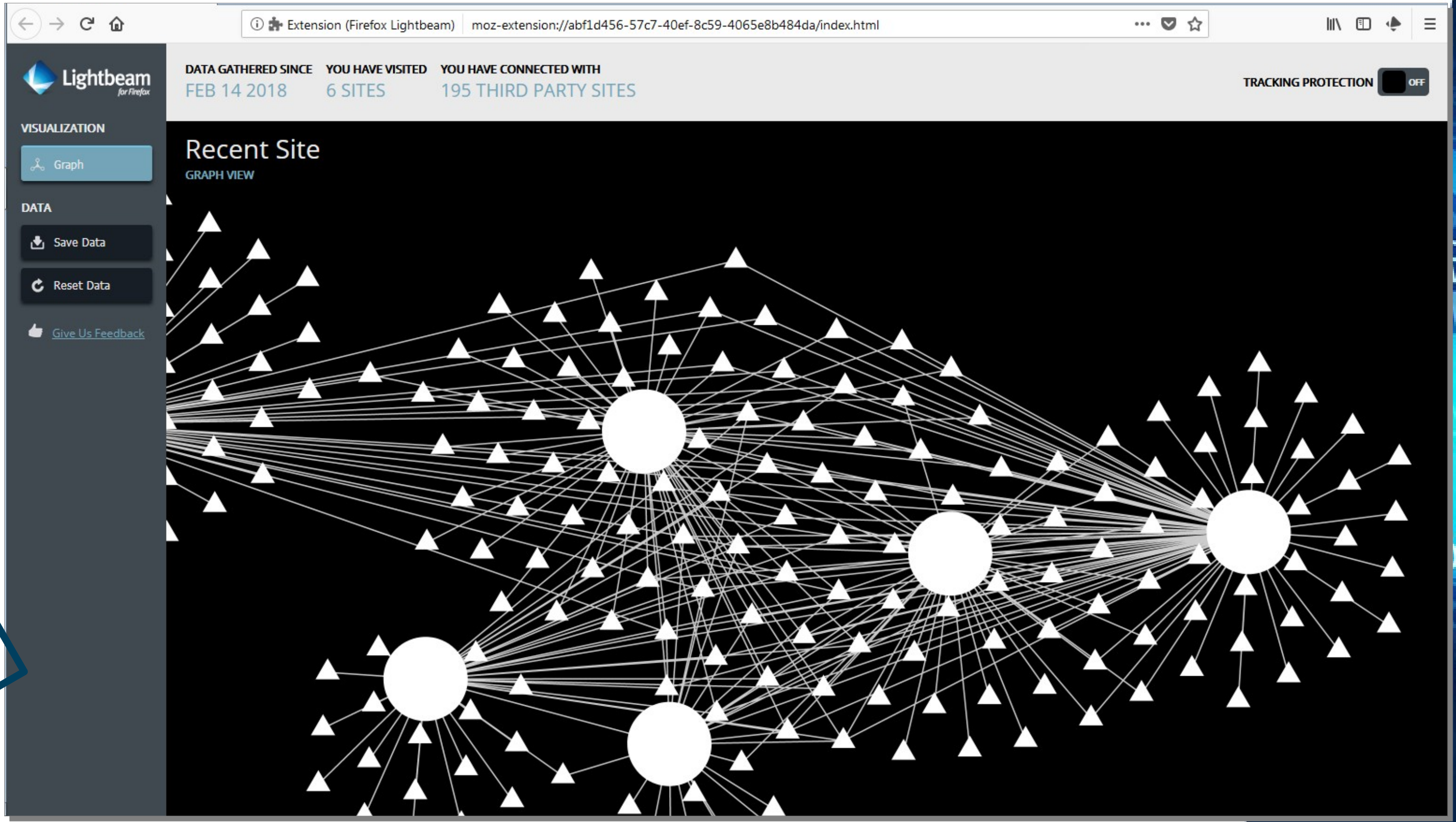
Subject's window inactive for one minute.

Subject's window inactive for thirty seconds.
Subjects average cursor spe[illegible]pared to all other subjects.
Ivory milestone: Subject has been on website for 1 min.

Subject has been pressing the button for ten seconds.
Subject has hovered above the button for ten seconds.
Subject's clicks are shorter than most other subjects.
Subject has been pressing the button for two seconds.

Tracking Live Demonstration: Lightbeam

- Visualizing add-on for Firefox, Chrom* (Thunderbeam-Lightbeam)
  - Big circles: directly reached sites (through clicks, entering URL in address bar)
  - Small triangles: Content loaded indirectly



Extension (Firefox Lightbeam) moz-extension://abf1d456-57c7-40ef-8c59-4065e8b484da/index.html

DATA GATHERED SINCE FEB 14 2018

YOU HAVE VISITED 6 SITES

YOU HAVE CONNECTED WITH 195 THIRD PARTY SITES

TRACKING PROTECTION OFF

Demo

Effects of Tracking

- User becomes more susceptible to manipulation
  - Wanted effect with regards to sales & advertising
  - But can be used for other manipulations too
- Loss of control over personal data through indifference
  - When Tracking/Surveilance is everywhere
- Power shifts away from users/consumers
- Accumulation of data in the hands of whom?
  - Their interests vs. the users/consumers interests?
- Slide towards a surveilance society
  - Knowledge of surveilance has stunting effects on free speech, etc.

Tracking through the Browser

- Browser features that leak personal/sensitive Information
  - ActivityStream (aka Startpage/Newtab)
  - Telemetry & Crashdumps
  - History & Cache
- Search Engines
- Cookies & Local Storage
- Browser Fingerprinting

Information leaks: Other

- Telemetry & Crashdumps
  - Send information home to Mozilla/Google/Microsoft/…
    - Usually not personal information, but allows tracking
  - May contain sensitive information (Crashdumps)
- History & Cache
  - Can be read/inferred through JavaScript from other sites
  - Can be limited/deleted through browser configuration
  - Can’t be prevented completely unless turned off completely

ActivityStream

- Privacy Problems:
  - Visiting the Startpage gives away IP-address and browser header/information to website operator
  - Displays advertising from vendor → tracking
  - Mousover over favorites page will trigger load of page
- Mitigations
  - Use empty Startpage or one from a trustworthy source
  - Turn of advertisements on startpage
  - Turn of pre-loading of favorites page

Search Engines

- By default: Bing (Edge), Google (most other browsers)
  - Tracking through Cookies, LocalStorage
- Tracking through URLs in search results:
  - Search engine displays: `https://example.com/somepage`
  - Real url: `https://www.google.com/url?q=https://example.com/somepage`
  - HTTP 302 redirect through search engine servers
- Pre-configured Search Engines append parameters to searches
  - …`&client=ubuntu` for Ubuntu
  - …`&rls=org.mozilla:de:official` for Downloads directly from Mozilla
  - Uninstall and re-install from web
  - Or edit search URL (Chrom*)

Search Engines: Mitigation

- Configure Alternative Search Engine that do less tracking
  - Qwant.com, Ixquick.com, DuckDuckGo.com, …
  - Meta Search Engines: Metager.de, Startpage.com, …
    - Use Google Index (among others)
    - Do not remove all tracking information
- Searches in popular sites can be done directly from search field
  - eg. Wikipedia, Stack Exchange, LEO, DeepL, etc.
  - Has to be configured as a search engine in the browser
- Add-on to remove tracking information from URLs
  - Neat URL, Skip Redirect, etc.
  - May break functionality if not configured carefully

Cookies

- Why?
  - HTTP is stateless
  - However, many applications need state information
    - Access tokens, settings, save points, highscores, etc.
  - Sent as part of the HTTP header
  - Created by JavaScript inside the browser
  - Or sent by the web server inside HTTP header
- The problem
  - Tracking across sessions and sites (except session cookies)
  - Most cookies are stored much longer than needed
  - Attackers may get access to sensitive/personal information (e. g. access tokens)

Local Storage

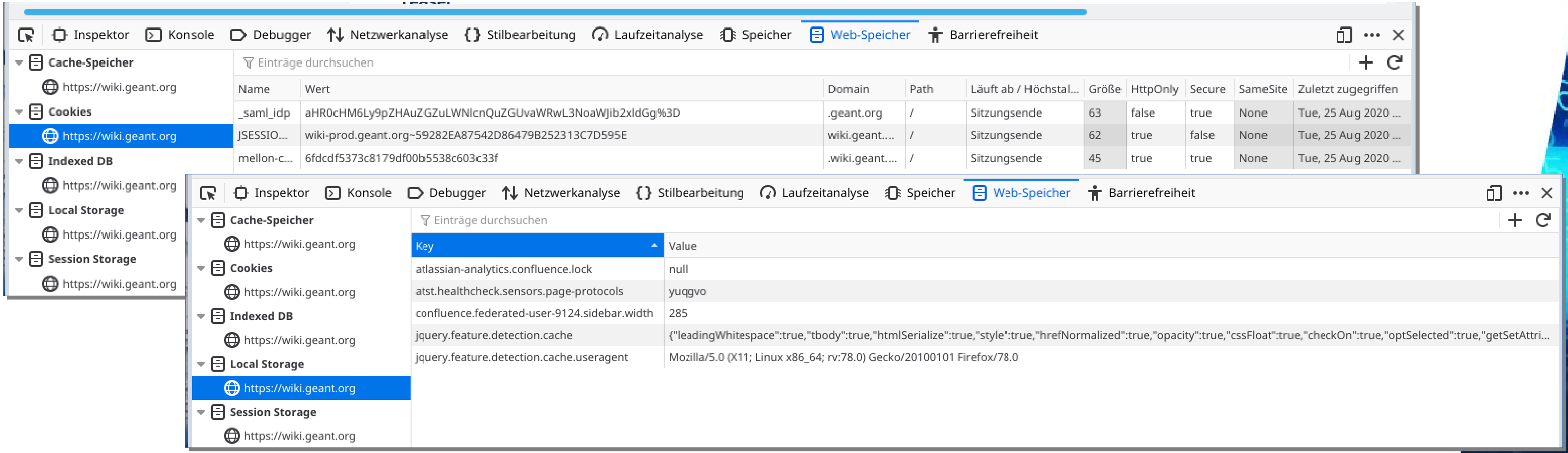
- Alias DOM-Storage
  - Used to be part of HTML 5, now its own W3C standard
  - Will be read or written locally by JavaScript (which is loaded from a website)
  - Will not be set as part of the HTTP header
  - Script may sent data within the limits of the same origin policy
- Local Storage: Persistent
- Session Storage: Non persistent (will be deleted when session ends)
- IndexedDB Storage: Persistence depends on calling application
  - Firefox only
  - WebSQL was W3C draft for other browsers (abandoned)

Flash Cookies & EverCookies

- Flash Cookies
  - Set by Flash applications
  - Stored in the Flash application folder
  - Gone with Flash for good (hopefully)
- EverCookies
  - Cookie will be regenerated from information in Flash Cookies or Local Storage via JavaScript

View Cookies & Local Storage

- Web Developer tools, Storage tab
- Shows all storage types: Cookies, Local Storage, IndexedDB, etc.



Name	Wert	Domain	Path	Läuft ab / Höchstal...	Größe	HttpOnly	Secure	SameSite	Zuletzt zugegriffen
_saml_idp	aHR0cHM6Ly9pZHAuZGZuLWNlcnQuZGUvaWRwL3NoaWJib2xldGg%3D	.geant.org	/	Sitzungsende	63	false	true	None	Tue, 25 Aug 2020 ...
JSESSIO...	wiki-prod.geant.org~59282EA87542D86479B252313C7D595E	wiki.geant....	/	Sitzungsende	62	true	false	None	Tue, 25 Aug 2020 ...
mellon-c...	6fdcdf5373c8179df00b5538c603c33f	.wiki.geant....	/	Sitzungsende	45	true	true	None	Tue, 25 Aug 2020 ...

Key	Value
atlassian-analytics.confluence.lock	null
atst.healthcheck.sensors.page-protocols	yuqgvo
confluence.federated-user-9124.sidebar.width	285
jquery.feature.detection.cache	{"leadingWhitespace":true,"tbody":true,"htmlSerialize":true,"style":true,"hrefNormalized":true,"opacity":true,"cssFloat":true,"checkOn":true,"optSelected":true,"getSetAttri...
jquery.feature.detection.cache.useragent	Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

Cookies & Local Storage Mitigation

- Blocking (not accepting) any Cookies → Many sites will not work
  - Esp. Captchas, Auth.-Servers, Session management
- Built-in Cookie Management
  - Treat all cookies as session cookies
  - Don’t accept third-party cookies
  - Affects both Cookies **and** LocalStorage
- Will still allow tracking until the browser is closed

Cookies & Local Storage Mitigation: Add-ons

- Cookie Management through add-ons:
- e.g. Cookie Auto Delete
  - Con: More work for the end-user (mistakes also happen)
    - Some add-ons track you too (e.g. Ghostery)
    - Redirects (esp authentication sites) can be a problem (configuration work)
  - Pro: More control and security
    - Selectively white-/blacklist Cookies/Local Storage entries
    - Deletion on tab-close, not browser-close
- Important: Use only one add-on or browser build-in blocking at a time!
  - i.e. “enhanced tracking protection” on Firefox
  - Can be a pain to find out which add-on is still blocking cookies

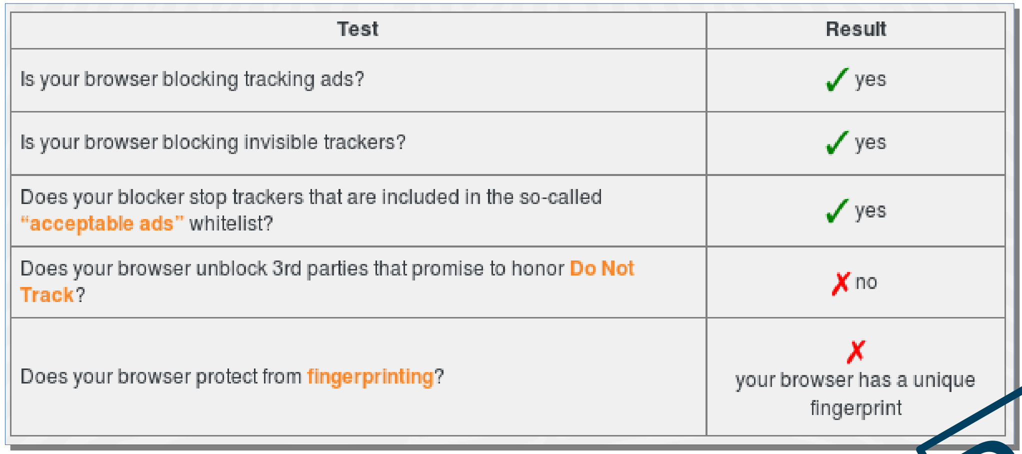
Tracking: Fingerprinting

- Idea: Collect enough information to (uniquely) identify system or user
  - Along with other information, like where you are
- Methods
  - HTTP Headers your browser sends
  - Canvas properties (size, etc.)
  - Installed set of fonts
  - Installed set of add-ons
  - Geolocation API
  - Every now and then, a new method is revealed
  - See `browserleaks.com` for more information

Tracking Live Demonstration: Browser Fingerprinting

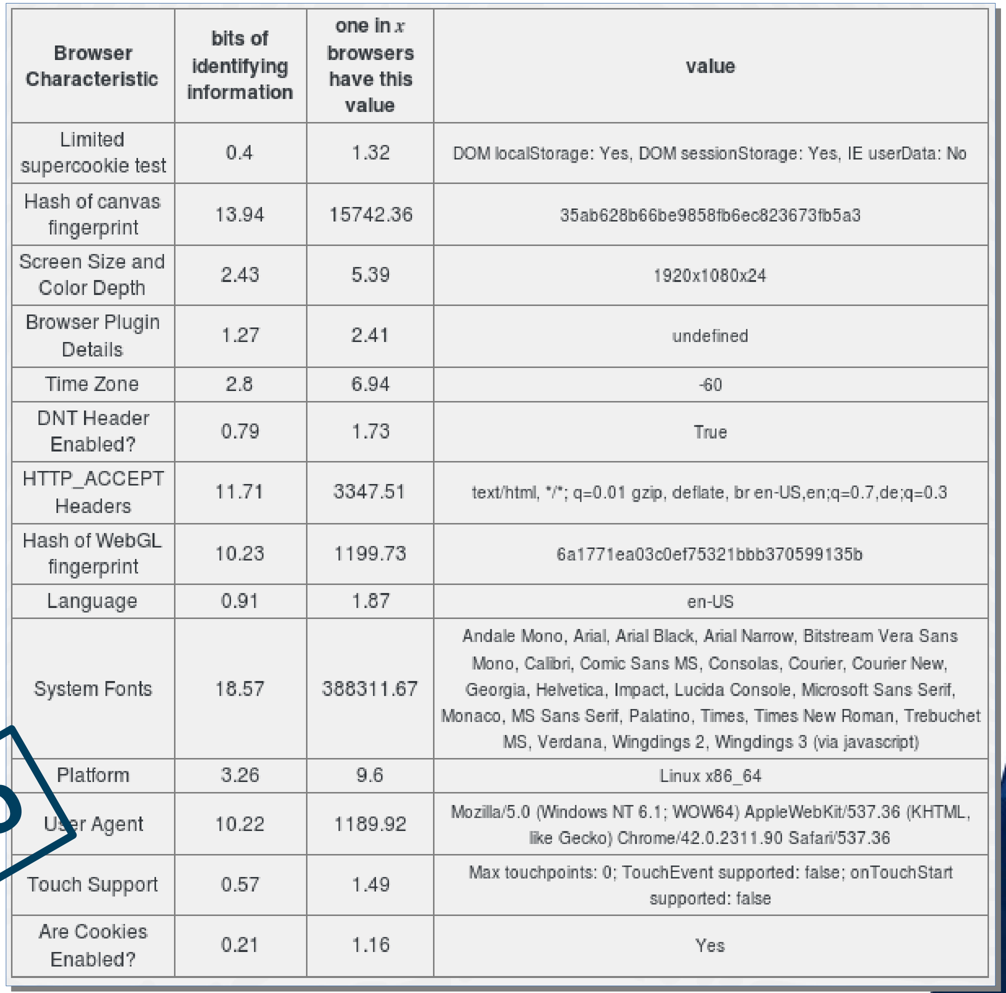
Test Sites:

- https://panopticlick.eff.org/
- https://browserleaks.com/



Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your blocker stop trackers that are included in the so-called "acceptable ads" whitelist?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Demo



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.4	1.32	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	13.94	15742.36	35ab628b66be9858fb6ec823673fb5a3
Screen Size and Color Depth	2.43	5.39	1920x1080x24
Browser Plugin Details	1.27	2.41	undefined
Time Zone	2.8	6.94	-60
DNT Header Enabled?	0.79	1.73	True
HTTP_ACCEPT Headers	11.71	3347.51	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.7,de;q=0.3
Hash of WebGL fingerprint	10.23	1199.73	6a1771ea03c0ef75321bbb370599135b
Language	0.91	1.87	en-US
System Fonts	18.57	388311.67	Andale Mono, Arial, Arial Black, Arial Narrow, Bitstream Vera Sans Mono, Calibri, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Console, Microsoft Sans Serif, Monaco, MS Sans Serif, Palatino, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.26	9.6	Linux x86_64
User Agent	10.22	1189.92	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36
Touch Support	0.57	1.49	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.16	Yes

Fingerprinting Mitigation

- Blocking 3rd Party JavaScript
  - Works as long as the fingerprinting is not done from the website itself or some site that is needed to function properly
- Add-ons
  - Block only specific tracking methods, like CanvasBlocker
  - Uninstalling unnecessary add-ons (Flash!) will block some techniques
- Disable Geolocation API
  - Practicable, except on mobile devices (maps, route-planing)

Stuff that does not work well

- Fake User-Agent HTTP header
  - Fingerprinting will still reveal your browser/OS
- Do Not Track (DNT)
  - Sending to advice to websites not to track
  - Sabotaged by adverstising companies & W3C
  - Nobody adheres to it
- Dedicated Tracking Blockers (add-ons)
  - eg. AdBlock, Disconnect, PrivacyBadger, Ghostery, Blockada, uBlock Origin, …
  - Generally do a nice job, however some cooperate with tracking services and whitelist trackers
  - uBlock Origin seems to work well

What have you learned?

- How to configure common browsers to
  - Minimize attack surface
  - Leave fewer traces
- And that it requires a major effort from users and admins

What has been left out?

- VPNs, TOR Network
- DNS, DNS over HTTPs – see upcoming course on DNS security
- WebRTC – see module on Videoconferencing Security & Privacy
- Lots of other stuff – see references/backup section

GÉANT
Networks • Services • People

Thank you

Any questions?

Next module: ***Email Privacy***, 21th of September 2020

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

References: General

- Browser vulnerabilities: `https://www.cvedetails.com/top-50-products.php`
- NoScript Tips: `https://www.privacypulp.com/5-tips-for-using-noscript/`
- Website analysis: `https://clickclickclick.click/`
- Browser fingerprinting: `https://panopticlick.eff.org/`
- More browser fingerprinting: `https://browserleaks.com/`
- JonDonym anonymity test: `https://ip-check.info/`
- Privacy Handbuch (German): `https://www.privacy-handbuch.de/`
- Mike Kuketz Blog (German): `https://www.kuketz-blog.de/`
- EFF Privacy page: `https://www.eff.org/issues/privacy`
- Privacy tools: `https://www.privacytools.io/`

References: TLS/SSL

- Windows Group Policy for TLS: https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#sslversionmin
- ENISA Algorithms, key size and parameters report 2014 https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
- Mozilla SSL Information: https://wiki.mozilla.org/Security/Server_Side_TLS
- Chromium SSL Information: https://www.chromium.org/Home/chromium-security/education/tls
- Information about SSL Certificate errors in browers: https://aboutssl.org/ssl-errors-by-browsers/
- Qualys SSL Labs Browser Test: https://www.ssllabs.com/ssltest/viewMyClient.html

Browser Extensions Mentioned

- NoScript: https://noscript.net/
- uMatrix: https://github.com/gorhill (Development put on hold 18th of September 2020)
- Lightbeam/Thunderbeam-Lightbeam: https://addons.mozilla.org/de/firefox/addon/lightbeam-3-0/
- Firefox Multi-Account Containers: https://addons.mozilla.org/de/firefox/addon/multi-account-containers
- Cookie Auto Delete: https://github.com/Cookie-AutoDelete/Cookie-AutoDelete
- CanvasBlocker: https://github.com/kkapsner/CanvasBlocker
- Canvas Blocker (Fingerprint protect): https://add0n.com/canvas-fingerprint-blocker.html
- Neat URL: https://addons.mozilla.org/de/firefox/addon/neat-url/
- Skip Redirect: https://addons.mozilla.org/de/firefox/addon/skip-redirect/
- Luminous: https://addons.mozilla.org/de/firefox/addon/luminous/
- Ublock Origin: https://github.com/gorhill/uBlock
- Blokada (iOS & Android only): https://blokada.org/
- Wappalyzer: https://addons.mozilla.org/de/firefox/addon/wappalyzer

Offline Analysis Tools

- Firefox Socorro: `https://github.com/mozilla-services/socorro`
- Breakpad: `https://chromium.googlesource.com/breakpad/breakpad`
- Nirsoft: MZCacheView, ChromeCacheView, IECacheView `https://www.nirsoft.com/`
- Chromagnon: `https://github.com/JRBANCEL/Chromagnon`

Backup material

Stuff that didn’t make it due to time constraints

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union’s Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

TLS Key Management & Identities

- I.e. Certificate Authorities
- For best security:
  - Empty shipped certficiate store and
  - Install only certificates you have personally verified
  - Might use an extra browser profile for high-security applications/sites (finances, medical, etc.)
  - Be careful with certificates that come from
  - Have to do this on organisations networks though, or we won’t have web access

Passwords

- Passwords stored in browser password store
  - Usually protected by Master password
  - In the past, there have been vulnerabilities
- Better: Dedicated password manager w/ browser add-on
  - Application/browser independent storage
  - On a dedicated medium for extra security & mobility
  - Deactivate browser passwort storage then
  - Depending on integration, may require additional copy-n-paste

Password Storage

- Storage in Firefox
  - `key3.db` – Master passwords and X.509 secret keys
  - `logins.json` – Password database (since FF 32)
    - Encryption: 3DE CBC
  - URLs and timestamps not encrypted

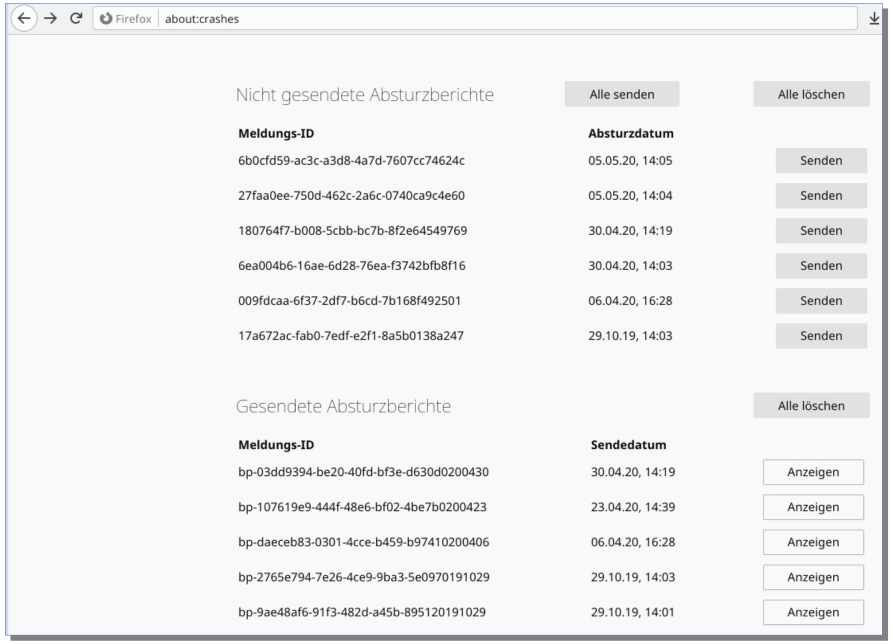
```
"id":1,
"hostname":"http://www.example.com/",
"httpRealm":null,
"formSubmitURL":"http://downloads.example.com/",
"usernameField":"userName",
"passwordField":"password",
"encryptedUsername":"XXXXXXXXXXXX",
"encryptedPassword":"XXXXXXXXXXXXX",
"guid":"{8be5cdad-b01d-490f-b003-c7fcdedd1e0b}",
"encType":1,
"timeCreated":1466569273228,
"timeLastUsed":1466569273228,
"timePasswordChanged":1466569273228,
"timesUsed":1
```

Telemetry

- Sending statistics about browser usage to Mozilla/Google/…
  - Optional, but opt-out
- View in browser
  - `about:telemetry`
  - `about:healthreport`
- On disk, directories
  - `datareporting`
  - `saved-telemetry-pings`
- Master switch
  - `Datareporting.policy.dataSubmissionEnabled=off`

Crash Reports

- Past crashes: `about:crashes`
- Sent reports are stored at Mozilla/Google/Microsoft/…
  - Minidump part is not publicly accessible (but sent nonetheless)

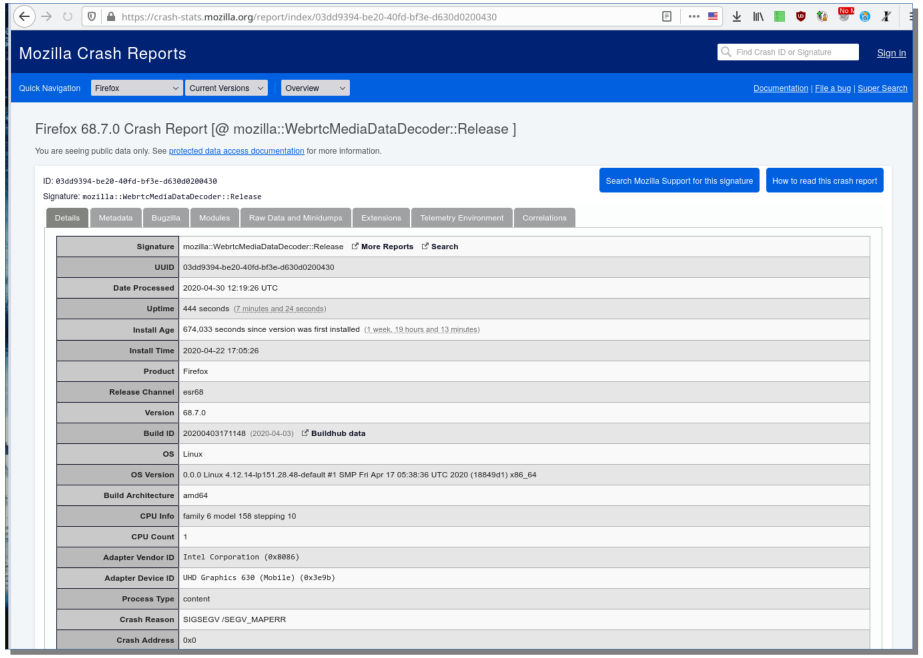


Nicht gesendete Absturzberichte

Meldungs-ID	Absturzdatum	
6b0cfd59-ac3c-a3d8-4a7d-7607cc74624c	05.05.20, 14:05	Senden
27faa0ee-750d-462c-2a6c-0740ca9c4e60	05.05.20, 14:04	Senden
180764f7-b008-5cbb-bc7b-8f2e64549769	30.04.20, 14:19	Senden
6ea004b6-16ae-6d28-76ea-f3742bfb8f16	30.04.20, 14:03	Senden
009fdcaa-6f37-2df7-b6cd-7b168f492501	06.04.20, 16:28	Senden
17a672ac-fab0-7edf-e2f1-8a5b0138a247	29.10.19, 14:03	Senden

Gesendete Absturzberichte

Meldungs-ID	Sendedatum	
bp-03dd9394-be20-40fd-bf3e-d630d0200430	30.04.20, 14:19	Anzeigen
bp-107619e9-444f-48e6-bf02-4be7b0200423	23.04.20, 14:39	Anzeigen
bp-daeceb83-0301-4cce-b459-b97410200406	06.04.20, 16:28	Anzeigen
bp-2765e794-7e26-4ce9-9ba3-5e0970191029	29.10.19, 14:03	Anzeigen
bp-9ae48af6-91f3-482d-a45b-895120191029	29.10.19, 14:01	Anzeigen


https://crash-stats.mozilla.org/report/index/03dd9394-be20-40fd-bf3e-d630d0200430
Mozilla Crash Reports
Find Crash ID or Signature
Sign in
Quick Navigation
Firefox
Current Versions
Overview
Documentation | File a bug | Super Search

Firefox 68.7.0 Crash Report [@ mozilla::WebrtcMediaDataDecoder::Release]

You are seeing public data only. See protected data access documentation for more information.

ID: `03dd9394-be20-40fd-bf3e-d630d0200430`

Signature: `mozilla::WebrtcMediaDataDecoder::Release`

Search Mozilla Support for this signature
How to read this crash report
Details
Metadata
Bugzilla
Modules
Raw Data and Minidumps
Extensions
Telemetry Environment
Correlations

Signature	mozilla::WebrtcMediaDataDecoder::Release **More Reports** **Search**
UUID	03dd9394-be20-40fd-bf3e-d630d0200430
Date Processed	2020-04-30 12:19:26 UTC
Uptime	444 seconds (7 minutes and 24 seconds)
Install Age	674,033 seconds since version was first installed (1 week, 19 hours and 13 minutes)
Install Time	2020-04-22 17:05:26
Product	Firefox
Release Channel	esr68
Version	68.7.0
Build ID	20200403171148 (2020-04-03) **Buildhub data**
OS	Linux
OS Version	0.0.0 Linux 4.12.14-lp151.28.48-default #1 SMP Fri Apr 17 05:38:36 UTC 2020 (18849d1) x86_64
Build Architecture	amd64
CPU Info	family 6 model 158 stepping 10
CPU Count	1
Adapter Vendor ID	Intel Corporation (0x8086)
Adapter Device ID	UHD Graphics 630 (Mobile) (0x3e9b)
Process Type	content
Crash Reason	SIGSEGV /SEGV_MAPERR
Crash Address	0x0

Crash Reports Mitigation

- Deactivate crash reports
  - Environment Variabls: MOZ_CRASHREPORTER_DISABLE=1
  - Configuration settings disable only the automatic uploading!
- Examination of reports
  - `https://crash-stats.mozilla.com/report/index/<ID>`
  - For Chrom*: Only when running your own crash report server
- Have your own Crash report server
  - Get Sourcecode from Socorro (Firefox) or Breakpad (Chrom*) page
  - Point your browser to it in the config: `breakpad.reportURL=https://crash.yourdom.example/`

Crash Reports on the hard disk

- `Crash Reports` directory in your browsers directory
  - `Pending`: not yet sent reports
  - `.dmp`: Minidump created by crashreporter(|.exe|.app) (Linux|Windows|Mac OS X)
    - Visual Studio Debugger (Windows)
    - `minidunp-2-core` (Linux), continue with gdb or other debugger
    - `breakpad` (for Chrom*)
  - .extra: JSON file with additional information: version, installed add-ons, linked libraries, etc.
  - `submitted`: sent reports
    - The prefix **`bp-`** is important, only then has the dump successfully been uploaded

Browser History

- Has many facettes
  - Browse history: where have you been
  - Download history: what have you downloaded
  - Forms history: what have you entered (in HTML forms)
  - Search history: what have you looked for
- Also
  - When (timestamps), from where (Referrer), how often, …
- Mitigations
  - Limit history through browser configuration settings
  - Use private browsing/Incognito mode

Browser Cache

- Cache in memory and on disk
- Cache on the hard disk can be read later
  - Index plus directories with data
- Directories can be searched with offline tools
  - Index evaluation tools: e.g. Nirsoft MZCacheView, ChromeCacheView, IECacheView, ChromagnonCache
- Mitigation
  - Cache on RAMdisk or tmpfs (Linux) – deletes cache at system restart
  - Use only the memory cache (Firefox: `cache.disk.enable = false`)
  - Delete Cache on Browser close
  - Performance impact usually neglectibly – many things can’t/won’t be cached

Cookies on the hard disk

- Firefox
  - `cookies.sqlite` - Cookies
  - `webappstorage.sqlite` - Local Storage
  - `storage/` - directory for indexedDB databases
- Chrom*
  - `Cookies` (without any suffix) but a Sqlite DB
  - `Local Storage/` - As single files (one for each data item)
- *EncryptedValue*: Encryption key is the users (master) password

Cookie Database Format

- Timestamp
  - 64 bit integer
  - Local time zone
- Firefox, Chrom*
  - Windows: Microseconds since 1st of January 1600, 00:00 UTC
    - Conversion inside Sqlite:

```
datetime(value / 1000000 + (strftime('%s', '1601-01-01')),
'unixepoch', 'localtime')
```

  - Unix/Linux: Microseconds since 1st of January 1970, 00:00 UTC
    - Conversion inside Sqlite:

```
datetime(value / 100000, 'unixepoch', 'localtime')
```

Private Browsing/Incognito Mode

- Firefox: private browsing, Chrom*: Incognito
- Main menu → Open new private/incognito window
- After activaton
  - Browser does not store History: Downloads, Forms, Pages, …
  - on disk or on users web account
  - Within the session, the data is available
  - No other effect with regards to security & tracking
    - OK, a little by one deleting cookies on tab-close, but: evercookies
- Useful on shared computers
  - If others should not see where you've been
  - Will deactivate plug-ins/add-ons unless enabled for private mode

Firefox Surf-Container

- Limit access to tracking data to sites from a Container
  - Define containers for specific activities or sites (i.e. work, private, banking, etc.)
- Two types: `FirstParty.Isolate` and `userContext`
- Both:
  - Data (cookies, cache, history, …) will be accessible within this container only
  - Does not help against tracking by browser-fingerprinting or IP-address
  - Does not otherwise improve security
  - Incompatible with Private Browsing Mode
- UserContext: Must be activated manually with each tab
  - Or by add-ons (e.g. Firefox Multi-Account Containers)
- FirstParty.Isolate: Each new sites gets a new container
  - Will break Single-Sign-On sites

Tracking via Accounts

- Many sites have you register for an account to access content
- Of course, you will be tracked & analyzed
  - Data is stored on operators servers
- However, this may go beyond the site
  - Site owner may have subsidiaries, sister companies, partners, etc.
  - Think about logging into sites with your social media account
- Technically, theres nothing we can do about it
- The operator has, under the GDPR to
  - Offer the provisions to move (your data) somewhere else
  - Answer your request about what personal information is stored about your account
  - Delete that data if you request so (and it is not needed)
- Recommendation: **GO AND ASK THEM!**