

PrivacyMachine – Zufälliger Fingerprint als Maßnahme gegen Webtracking

Einleitung:

Webtracking¹ wird heutzutage nicht nur mehr durch die Verwendung von Cookies erreicht, sondern es kommen wesentlich fortgeschrittenere Techniken wie Fingerprinting² zur Anwendung. Die OpenSource-Software PrivacyMachine stellt ein neues Konzept vor, welches Webtracking gezielt entgegenwirkt.

Wodurch entsteht dieser Fingerprint?

Die wichtigsten Eigenschaften des Fingerprints lassen sich per JavaScript auslesen und dienen ursprünglich dazu, dass sich eine Seite auf den verwendeten Browser anpassen kann.

Die Summe dieser Eigenschaften wie Bildschirmauflösung oder im Betriebssystem installierter Schriften ist jedoch einzigartig und ermöglicht ein Wiedererkennen eines Computers auf unterschiedlichen Seiten.

Die eleganteste Lösung wäre nun per JavaScript so wenig Information wie nötig auszulesen und dies zu standardisieren. Die Entwicklung eines konkurrenzfähigen modernen Browsers ist jedoch aufgrund der notwendigen Geldmittel nur mehr großen Konzernen möglich.

Bisherige Ansätze gegen Webtracking versuchen eine möglichst große Gruppe an Usern zu schaffen, die den selben Fingerprint beim Surfen verwenden. Dadurch ist ein einzelner User in der Gruppe nicht mehr identifizierbar.

Ein sehr ausgereiftes Beispiel für diesen Ansatz stellt der TOR-Browser dar.

Folgende Seiten berechnen die Einzigartigkeit des Fingerprints und stellen diesen dar:

<https://panopticlick.eff.org>

<https://amiunique.org>

Man kann auf diesen Seiten gut erkennen, dass es ohne radikale Maßnahmen wie ausgeschaltetem JavaScript kaum möglich ist, in eine Gruppe relevanter Größe zu fallen.

Die meisten Browserinstallationen sind einzigartig.

Durch Aktivieren von Gegenmaßnahmen, welche meist durch die Installation von mehreren Browser-Plugins erreicht werden, entstehen zwei Effekte:

- Die Benutzbarkeit der Seiten ist extrem eingeschränkt, weil eine Vielzahl von individuellen Optionen für eine Seite erst manuell freigeschalten werden muss, damit diese funktioniert (Beispiel: NoScript)
- Mit jedem installierten Plugin verschlechtert sich die Anonymität, weil die Liste der installierten Plugins Teil des Fingerprints ist.

1 „Webtracking“ ist das Wiedererkennen des Benutzers auf unterschiedlichen Webseiten.

2 Ein „Fingerprint“ ist die Summe der Eigenschaften eines Computers die diesen Computer einzigartig machen.

Was ist neu am Konzept der PrivacyMachine?

Die PrivacyMachine wirkt für den Benutzer wie ein normaler Browser, mit dem Unterschied, dass hinter jedem Tab eine eigene virtuelle Maschine läuft, die den Inhalt eines Standard-Browsers anzeigt. Jede virtuelle Maschine erhält per VPN oder TOR eine eigene IP-Adresse.

Dies hat den Vorteil, dass beim Schließen des Tabs die Maschine auf einen Snapshot zurückgesetzt wird → Alle Arten von Cookies wie Flash-Cookies oder Browser-Local-Storage werden gelöscht. Weiters wird der Fingerprint verändert, indem die Eigenschaften des Betriebssystems und der installierten Software geändert werden. Diese Eigenschaften bilden den Großteil des Fingerprints, welche der Browser per JavaScript ausliest und an die Domains der Webtracker sendet.

**Bei jedem Öffnen eines Tabs wird so ein neuer einzigartiger Fingerprint erzeugt.
Der User kann parallel mit zwei verschiedenen Fingerprints surfen.**

Kann man nun nicht den User aufgrund des „sehr einzigartigen“ Fingerprints wiedererkennen?

Das ist richtig, wenn es nur einen User gibt, aber die Implementierung der Erkennung eines einzelnen Users macht für die Trackinganbieter ökonomisch keinen Sinn.

Wenn aber eine Gruppe von z.B. 20 Personen die PrivacyMachine verwenden, können die einzelnen Nutzer voneinander nicht mehr unterschieden werden und das gemittelte Personenprofil macht entweder keinen Sinn -- wechselndes Geschlecht und wechselndes Alter -- oder bildet ein Summen-Profil wie z.B. die Leser eines Print-Mediums → **Den Benutzern wird nur mehr nichtpersonalisierbare Werbung eingeblendet, und das Erstellen von umfassenden Personenprofilen wird unterbunden.**

Hier ein Screenshot von zwei Fingerprints zweier gleichzeitig geöffneter VM-Masken(=virtuelle Maschinen) von <https://panopticklick.eff.org>

PrivacyMachine

Menu

Fingerprint_01 x Fingerprint_02 x +

Panopticklick x +

https://panopticklick.eff.org/results?&a=111

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.42	1.34	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	14.9	30563.33	b7836a263f2f58b41f33b4aeb44c5b6b
Screen Size and Color Depth	17.48	183380.0	720x668x24
Browser Plugin Details	1.78	3.42	undefined
Time Zone	8.25	305.12	-600
DNT Header Enabled?	1.21	2.31	False
HTTP_ACCEPT Headers	2.5	5.66	text/html,*/*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	2.33	5.03	00000000000000000000000000000000
Language	13.58	12225.33	eo
System Fonts	9.49	719.14	Bitstream Vera Sans Mono, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.12	8.72	Linux x86_64
User Agent	6.2	73.44	Mozilla/5.0 (X11; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0
Touch Support	0.5	1.41	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.15	Yes

"Fingerprint_01" - Locale: eo, Time Zone: Pacific/Saipan, Additional Fonts: 6/3001, External IP: 188.172.217.53, Screen Size: 720x668

PrivacyMachine

Menu

Fingerprint_01 x Fingerprint_02 x +

Panopticklick x +

https://panopticklick.eff.org/results?&a=111

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.42	1.34	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	11.7	3334.24	80b3fc8bbd9dcb22193c2a8a421c5beb
Screen Size and Color Depth	17.48	183383.0	720x672x24
Browser Plugin Details	1.78	3.42	undefined
Time Zone	7.86	233.02	-540
DNT Header Enabled?	1.21	2.31	False
HTTP_ACCEPT Headers	3.78	13.75	text/html,*/*; q=0.01 gzip, deflate en-US,en;q=0.5
Hash of WebGL fingerprint	2.33	5.03	00000000000000000000000000000000
Language	8.75	429.47	cs
System Fonts	9.48	716.34	Bitstream Vera Sans Mono, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.12	8.72	Linux x86_64
User Agent	6.28	77.67	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Touch Support	0.5	1.41	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.15	Yes

"Fingerprint_02" - Locale: cs_CZ, Time Zone: Pacific/Palau, Additional Fonts: 3/3001, External IP: 185.20.99.141, Screen Size: 720x672

Autoren: Bernhard Zach, Olaf Pichler, Alexander Leopold

contact@privacymachine.eu

OpenPGP-Fingerprint: 0C93 F15A 0ECA D404 413B 5B34 C6DE E513 0119 B175

This work is licensed under the „Creative Commons Attribution-ShareAlike 4.0 International License“

<http://creativecommons.org/licenses/by-sa/4.0/>