Javascript, Browserfingerprinting und Webtracking

Oder:
Unsichtbare Mächte beobachten uns ...
besonders bei aktiviertem Javascript

Arno “Mr. X” Nuehm

an.to_n-73 at riseup dot net

0B4C DF2C CB22 5DF4 25EA F212 49D1 ABF2 A2A9 7D7D

2014-08-31, Show & Tell Realraum Graz

- Webtracking ist ein grosses Geschäft

- Webtracking Report 2014, Fraunhofer Institut
https://www.sit.fraunhofer.de/wtr
Zusammenfassung S. 7 – 16

- Nutzerdaten als “Rohstoff”: *Alter, Ausbildung, Beruf, Einkommen, Ethnie, Drogenkonsum, Familienstand, Geschlecht, Geschmack, Gesundheitszustand, Hobbies, Interessen, Konsumverhalten, Meinung, Namen, politische Einstellung, Religionszugehoerigkeit, Risikobereitschaft, Schwangerschaft, sexuelle Orientierung, soziale Verflechtung, Sprachfertigkeit, Trinkgewohnheiten, Vorlieben, Wohnort*

- “Targeted Advertising” ist effizienter als ungerichtete Werbung
Webtracking ist nur ein Teil des Problems (Kundenkarten etc.)

→ Wir sind in der Totalüberwachungs längst angekommen! Kommerziell und staatlich.

- “Dann wissen die eben alles, wo ist das Problem?”
“Ich habe nichts zu verbergen!”

- Wahlbeeinflussung, US Demokraten 2012
  Inside the Secret World of the Data Crunchers Who Helped Obama Win, Scherer M., 2012-11-07
http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-
  Wir wissen, wen Du wählen wirst, Schulz S., 2013-08-31
http://www.faz.net/aktuell/feuilleton/wie-big-data-das-wahlgeheimnis-aush

- Verkauf Personenprofile an Krankenversicherung
  Everything We Know About What Data Brokers Know About You, Beckett L., 2014-06-13
http://www.propublica.org/article/everything-we-know-about-what-data-br

- Potentielle Datenkunden: Kreditgeber, Arbeitgeber

Webtracking

Der Klassiker: 3rd Party Cookies

Etwas fortgeschritten: Flash Cookies (Local shared objects – LSOs)

Wahlloses Probesurfen auf populären Seiten, z. B. https://www.youtube.com , http://www.gamezone.de , http://www.zeit.de , http://www.krone.at , http://www.kleinezeitung.at

→ Viele 3rd Party Cookies gesetzt
→ Einige LSOs gesetzt

→ Ohne regelmaessiges Loeschen wird die Sammlung immer größer und die eigene Verfolgbarkeit besser

- Lokal gespeicherte Kenner kann man löschen (Cookies, LSOs, Cache, HTML5 Cookies ...)
    Im Firefox selber
    Mit Löschprogrammen http://bleachbit.sourceforge.net

Browser-Fingerprinting:
Teilweises Auslesen der Konfiguration von Browser und Betriebssystems → Weltweit einmalige Kombination

→ Geht am besten per Javascript!

Ein paar Testseiten:
https://panopticlick.eff.org

http://letmetrackyou.org/identify.php

http://browserspy.dk

Wer macht denn sowas?

Fingerprinting Category	Panopticlick	BlueCava	Iovation ReputationManager	ThreatMetrix
Browser customizations	Plugin enumeration$_{(JS)}$ Mime-type enumeration$_{(JS)}$ ActiveX + 8 CLSIDs$_{(JS)}$	Plugin enumeration$_{(JS)}$ ActiveX + 53 CLSIDs$_{(JS)}$ Google Gears Detection$_{(JS)}$		Plugin enumeration$_{(JS)}$ Mime-type enumeration$_{(JS)}$ ActiveX + 6 CLSIDs$_{(JS)}$ Flash Manufacturer$_{(FLASH)}$
Browser-level user configurations	Cookies enabled$_{(HTTP)}$ Timezone$_{(JS)}$ Flash enabled$_{(JS)}$	System/Browser/User Language$_{(JS)}$ Timezone$_{(JS)}$ Flash enabled$_{(JS)}$ Do-Not-Track User Choice$_{(JS)}$ MSIE Security Policy$_{(JS)}$	Browser Language$_{(HTTP, JS)}$ Timezone$_{(JS)}$ Flash enabled$_{(JS)}$ Date & time$_{(JS)}$ Proxy Detection$_{(FLASH)}$	Browser Language$_{(FLASH)}$ Timezone$_{(JS, FLASH)}$ Flash enabled$_{(JS)}$ Proxy Detection$_{(FLASH)}$
Browser family & version	User-agent$_{(HTTP)}$ ACCEPT-Header$_{(HTTP)}$ Partial S.Cookie test$_{(JS)}$	User-agent$_{(JS)}$ Math constants$_{(JS)}$ AJAX Implementation$_{(JS)}$	User-agent$_{(HTTP, JS)}$	User-agent$_{(JS)}$
Operating System & Applications	User-agent$_{(HTTP)}$ Font Detection$_{(FLASH, JAVA)}$	User-agent$_{(JS)}$ Font Detection$_{(JS, FLASH)}$ Windows Registry$_{(SFP)}$	User-agent$_{(HTTP, JS)}$ Windows Registry$_{(SFP)}$ MSIE Product key$_{(SFP)}$	User-agent$_{(JS)}$ Font Detection$_{(FLASH)}$ OS+Kernel version$_{(FLASH)}$
Hardware & Network	Screen Resolution$_{(JS)}$	Screen Resolution$_{(JS)}$ Driver Enumeration$_{(SFP)}$ IP Address$_{(HTTP)}$ TCP/IP Parameters$_{(SFP)}$	Screen Resolution$_{(JS)}$ Device Identifiers$_{(SFP)}$ TCP/IP Parameters$_{(SFP)}$	Screen Resolution$_{(JS, FLASH)}$

aus:
Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting, Nikiforakis N., 2013-05
https://www.cs.ucsb.edu/~vigna/publications/2013_SP_cookieless.pdf

- Vorläufige Entwarnung:
Verwendung bisher nur auf ca. 6 % der populären Seiten

Searching for Indicators of Device Fingerprinting in the JavaScript Code of Popular Websites, Rausch M., 2014-04 , US Top 1000, Quantcast
http://www.micsymposium.org/mics2014/ProceedingsMICS_2014/mics20

The Web never forgets: Persistent tracking mechanisms in the wild, Acar G., 2014-08, Global Top 100000, Alexa
*https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_*

Aber: Das wird mehr werden!
→ Aufmerksamkeit für Tracking steigt
→ Immer mehr Leute schalten Cookies ab.
→ Tracker suchen Alternativen

Wettlauf zwischen Trackern und Nutzern geht in die nächste Runde ….

- Beispiele Fingerprinting auf Probeseiten mittels NoScript
  NoScript kontrolliert alle 1st und 3rd Party Scripts
  http://noscript.net

Probleme Fingerprinting:
- Kann nur mit Detailanalyse Datenstrom entdeckt werden, fortgeschrittene IT Kenntnisse norwendig

- Abwehrmassnahme mit aktiviertem JS sehr schwierig

Beispiele
  ProPublica
http://www.propublica.org/article/meet-the-online-tracking-device-that-is-v
  EFF → whitehouse.gov
https://www.eff.org/deeplinks/2014/07/white-house-website-includes-uniq

- 1st-party Scripts können nicht abgewehrt werden auf Seiten, die nur mit JS funktionieren **==> Javascript ggf. Komplett abschalten**