**Online Tracking**

**Types of tracking**

* Cookies
* Super cookies
* Ad networks
* Email provider
* ISP (DNS queries)
* Mobile network provider
* Governments
* Work, uni, school
* Shared WiFi
* Radio

**IP Address**

Any connection of made on the internet (TCP) will require you to reveal your IP

**3rd party connections**

**HTTP referrer**

* In http header

When you click a link, the http referrer tells the visited webpage where out came from

If the webpage includes an ad, then there will be referrer in there telling the ad p[provider where you came from

**Conversion pixels**

* 1x1 pixels that use http referrers that can track you
* Invisible on a website
* Can also be used in emails, will track loading and use of that email

**Cookies & Scripts**

* Small bits of information sent and stored by browser
* Browser then send this to each website with every request so the website knows you are the same person
* Store selected settings and logins etc (session cookies)

If two websites use the same cookies (like double-click cookies) then they will both know that you’ve visited each website

If a cookie is captured by a MITM then the cookie can be relayed back into the HTTP header and login in as you

* This is why it’s important to make sure cookies are sent over an encrypted HTTPS connection
* This prevents cookies being injected and/or taken out

**Super Cookies**

General term for methods to permanently track a user

Can’t be deleted in the same fashion a regular cookie can be

**Evercookie**

Local shared objects (flash cookies)

Silverlight isolated storage

Storing cookies in web history, HTTP Etags, web cache etc.

Window.name chaching

IE userData storage

HTML5 session, local and database storage (via SQLite)

HTML 5 Indexed Database

Exploits

* Java JNLP persistence service
* Java CVE-2013-0422 (sandbox escaping)

When a browser notices part of the super cookie has been deleted (e.g., web history cookies), the deleted part will be repopulated from the other locations like using flash cookies

Cookies that are recreated after deleting from backup stored locations outside the browsers dedicated cookie store are call **Zombie Cookies**

**‘The Rise of Mobile Tracking headers: How Telcos around the world are threatening your privacy**

Using an encrypted connection via HTTPS can mitigate cookie injection into HTTP headers as the connection would have to be decrypted first

**Browser Fingerprinting**

**Panopticlick** is a website that shows you what fingerprinting info your browser hold

**Ipleak.net** as well

**Browser Functionality**

**Geolocation**

* Most browsers give out geolocation data to obtain ‘optimised’ search results and give to other websites etc.
* Browserleaks.com can show you what info is being given up

**Safe browsing and phishing protection**

* Beacon out any website that you visit in order to scan for potential malware or attacks

**Sendpings**

**WebTRC**

**Extensions and Plugins**

* Could be becaoning out to the creator or other parties

**HTML canvasing (JavaScript)**

**Browser History**

**Operating systems**

**Applications and software**

* Can easily send out data

**Security applications**

* Anti virus

**Malware (keyloggers, RATs, Trojans)**

**Network Devices (Routers, Switches, Firwalls etc.)**

**DNS**

* Queries can be logged by whoever they’re being sent to I.e., IPS
* DNS leaking when queries are sent through normal unencrypted network instead of through secure tunnel
* DNS address detection

**Auto updates**

* Applications always making connections to find new updates

**Any automatic connections**

**Error reports**

* Connections to developers

**User Profiling**

The profile that mass surveyors create on a person based off of their internet usage

* Like in the social dilemma

Presence events and Target detection identifiers

This is possible only if traffic passes through equipment that ‘they’ own

* Needs to be an adversary with sufficient power i.e., nation state or GCHQ (UK)
* Using probes into fibre optic cables
* A lot of international traffic actually goes through the UK cables