**Browser Fingerprinting & HTTP Referrer**

**HTTP Refferer**

Is a http header

* Browser loads the webpage and tell the website where you’ve come from
* Also sent when loading content on a webpage like ads or tracking scripts
  + They will know which page you are viewing

Referrer spoofing allows you to control this

**RefControl**

* Allows you to control what gets sent as a HTTP referrer on a per site basis

**Smart Referrer**

* Will only send referrers when staying on the same domain

**Firefox**

* About:config
* Network.http.sendRefererHeader
  + Set value to 0 to disable referrer

**uMatrix**

* Spoof referrer string

**Browser Fingerprinting**

**Browsers automatically send information about its settings and preferences to websites**

* User agent
* Browser type
* Add-ons
* Sites can query browser to get more info

**If settings are unique enough, then fingerprinting can be done**

Cookies aren’t needed for this

Studies found that **84% of browsers have a unique fingerprint**

And of those that have **Java** and **Flash** enabled, **94%**

* Again, not including cookies to fingerprint

**Objects used to fingerprint (not exhaustive)**

* *Plugins*
* HTML5 Canvas Image Extraction
* Open TCP Port and Local Network Fingerprinting
* Invasive Authentication Mechanisms (NTLM and SPNEGO)
* USB Device ID Enumeration via GamePad API
* Fonts
* Monitor, Widget and OS Desktop Resolution
* Display Media Information
* WebGL
* User Agent and HTTP Headers
* Locale Fingerprinting
* Time-zone and Clock Offset
* JS Performance Fingerprinting
* Keystroke Fingerprinting
* OS Type Fingerprinting

**Browserleaks.com/flash**

**Ipleaks.com**

* Shows what information sites can get from querying the browser through plugins and Flash, JS etc.

**User Agents and HTTP Headers**

Random Agent Spoofer (Plugin)

* Randomise user agent or specifically select one

Your User Agent can also be enumerated from the DOM object navigator.userAgent

* JS will query this
* Will also have to be changed
* Which it does

**HTML5 Canvas Image Extraction**

Canvas is a HTML5 element which is used to draw graphics animation on a webpage via scripting in JS

* Can also be used in fingerprinting
* Based on the idea that the same canvas image may be rendered different in different computers

**CanvasBlocker**

* Blocks JS canvas API from fingerprinting browser

**Open TCP Port and Local Network Fingerprinting**

In Firefox, by using WebSockets or XHR, its possible for remote content to enumerate open ports

**Panopticlick**

* Tester to show uniqueness of browser

**Tor browser** is the best hardened browser with code in the back end to mitigate fingerprinting

**JonDoFox**

* Hardened browser for uniformity

**Virtual Machines and default browsers**

**Live OS**

* Uniformity