Real browser fingerprinting in 2017

GreHack 2017

Antoine Vastel - University of Lille/INRIA

Outline

1. What is browser fingerprinting?
2. Why is it used?
3. How is it used?

What is browser fingerprinting?

History

Stateless tracking technique
Discovered in 2010 by Eckersley

Relies on diversity of:

1. OS
2. Browsers
3. Devices

Example of a fingerprint

Attribute	Value
User agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.86 Safari/537.36
Languages	fr-FR,fr;q=0.8,en-US;q=0.6,en;q=0.4

Accept	text/html,application/xhtml+xml,applicati q=0.9,image/webp,image/apng,*/*;q=0.8
Encoding	gzip, deflate, br
Plugins	Plugin 0: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai. Plugi Chrome PDF Viewer; Portable Document Format; internal-pdf-viewer. Plugin 2: Nat Client; ; internal-nacl-plugin.

Platform	Linux x86_64
Cookies	yes
Timezone offset	-120
Screen resolution	1280x720
Fonts	List of fonts

Statistics

83.6% of fingerprints were unique

94.2% if Flash activated

Why use fingerprinting?

For advertising

> *There ain't no such thing as a free lunch.*

Content producers don't work for free.

Profile of interests

Assign a unique user id to build profiles.

Alternative or support (regenerate) to classical cookies.

For security

Fraudsters don't keep cookies

How much is it used?

Statistics from *"Online Tracking: A 1-million-site Measurement and Analysis"* by Englehardt and al:

More than 5% of top 1k Alexa

Research on fingerprinting

New attributes

- Audio, Canvas fingerprinting
- JS fonts enumeration
- JS Engine fingerprinting
- 3D shapes rendering with WebGL

Academia vs Industry

What's good in theory may not be exploitable in practice

Some techniques are too slow:

- Complex 3D shapes rendering with WebGL
- "Exhaustive" fonts enumeration
- JS engine fingerprinting

Current state of browser fingerprinting in the wild

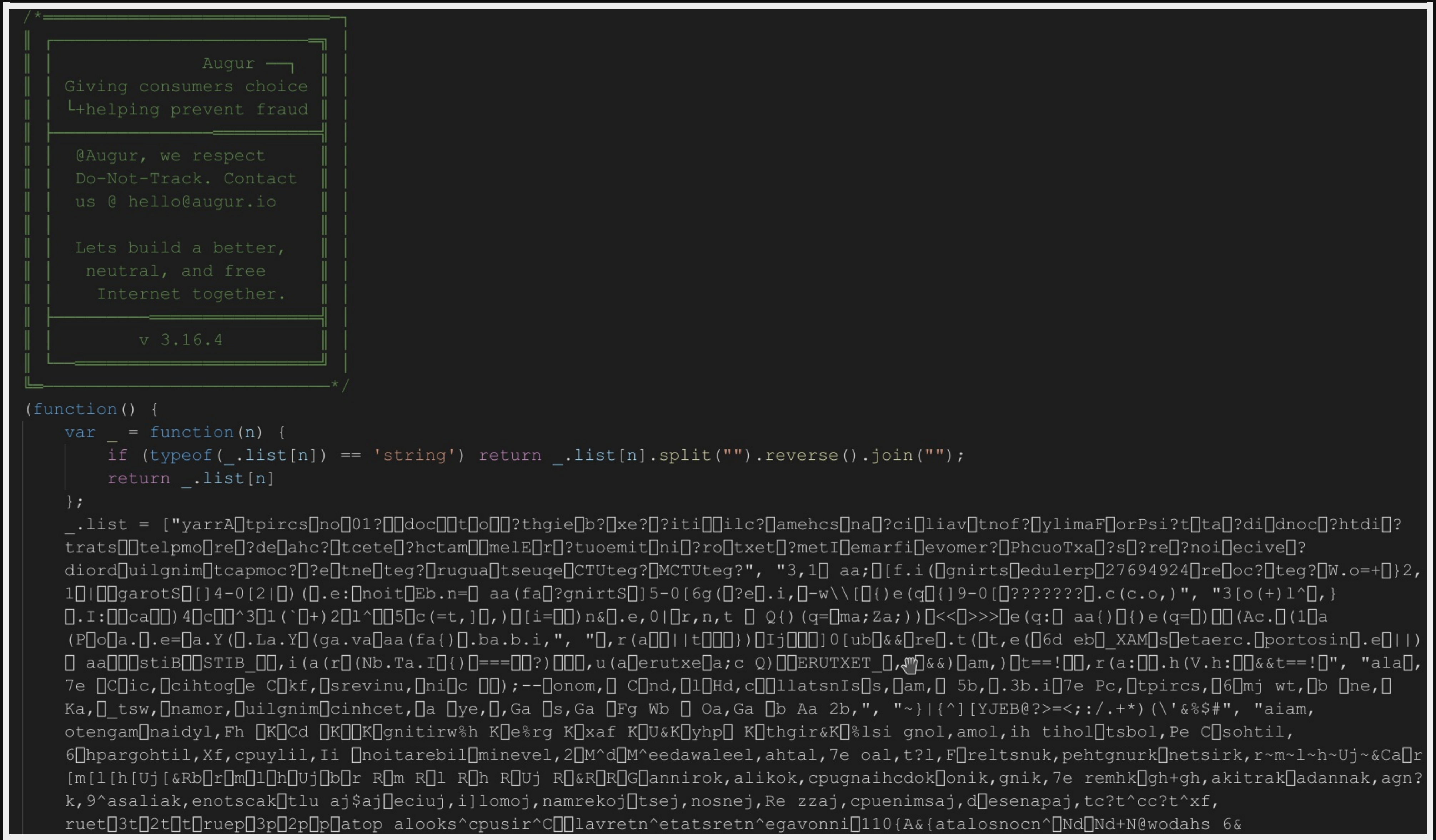
Two cases:

1. Advertising/Marketing: Augur
2. Security: Perimeterx

What's really used?

Augur

Script



```
/*═══════════════════════════════════════════════════╗
║  ┌──────────────────────────────────────────────╖  ║
║  │                    Augur ─┐                  ║  ║
║  │ Giving consumers choice  ║  ║
║  │  └+helping prevent fraud ║  ║
║  ├──────────────────────────────────────────────╢  ║
║  │  @Augur, we respect      ║  ║
║  │  Do-Not-Track. Contact   ║  ║
║  │  us @ hello@augur.io     ║  ║
║  │                          ║  ║
║  │  Lets build a better,    ║  ║
║  │   neutral, and free      ║  ║
║  │    Internet together.    ║  ║
║  ├──────────────────────────────────────────────╢  ║
║  │        v 3.16.4          ║  ║
║  └══════════════════════════════════════════════╝  ║
╚════════════════════════════════════════════════════*/
(function() {
    var _ = function(n) {
        if (typeof(_.list[n]) == 'string') return _.list[n].split("").reverse().join("");
        return _.list[n]
    };
    _.list = ["yarrA□tpircs□no□01?□□doc□□t□o□□?thgie□b?□xe?□?iti□□ilc?□amehcs□na□?ci□liav□tnof?□ylimaF□orPsi?t□ta□?di□dnoc□?htdi□?
    trats□□telpmo□re□?de□ahc?□tcete□?hctam□□melE□r□?tuoemit□ni□?ro□txet□?metI□emarfi□evomer?□PhcuoTxa□?s□?re□?noi□ecive□?
    diord□uilgnim□tcapmoc?□?e□tne□teg?□rugua□tseuqe□CTUteg?□MCTUteg?", "3,1□ aa;□[f.i(□gnirts□edulerp□27694924□re□oc?□teg?□W.o=+□}2,
    1□|□□garotS□[]4-0[2|□)(□.e:□noit□Eb.n=□ aa(fa□?gnirtS□]5-0[6g(□?e□.i,□-w\\[□{)e(q□{]9-0[□???????□.c(c.o,)", "3[o(+)1^□,}
    □.I:□□ca□□)4□c□□^3□1(`□+)2□1^□□5□c(=t,]□,)□[i=□□)n&□.e,0|□r,n,t □ Q{)(q=□ma;Za;))□<<□>>>□e(q:□ aa{)□{)e(q=□)□□(Ac.□(1□a
    (P□o□a.□.e=□a.Y(□.La.Y□(ga.va□aa(fa{)□.ba.b.i,", "□,r(a□□||t□□□})□Ij□□□]0[ub□&&□re□.t(□t,e(□6d eb□_XAM□s□etaerc.□portosin□.e□||)
    □ aa□□□stiB□□STIB_□□,i(a(r□(Nb.Ta.I□{)□===□□?)□□□,u(a□erutxe□a;c Q)□□ERUTXET_□,□□&&)□am,)□t==!□□,r(a:□□.h(V.h:□□&&t==!□", "ala□,
    7e □C□ic,□cihtog□e C□kf,□srevinu,□ni□c □□);--□onom,□ C□nd,□1□Hd,c□□llatsnIs□s,□am,□ 5b,□.3b.i□7e Pc,□tpircs,□6□mj wt,□b □ne,□
    Ka,□_tsw,□namor,□uilgnim□cinhcet,□a □ye,□,Ga □s,Ga □Fg Wb □ Oa,Ga □b Aa 2b,", "~}|{^][YJEB@?>=<;:/.+*)(\'&%$#", "aiam,
    otengam□naidyl,Fh □K□Cd □K□□K□gnitirw%h K□e%rg K□xaf K□U&K□yhp□ K□thgir&K□%lsi gnol,amol,ih tihol□tsbol,Pe C□sohtil,
    6□hpargohtil,Xf,cpuylil,Ii □noitarebil□minevel,2□M^d□M^eedawaleel,ahtal,7e oal,t?l,F□reltsnuk,pehtgnurk□netsirk,r~m~l~h~Uj~&Ca□r
    [m[l[h[Uj[&Rb□r□m□l□h□Uj□b□r R□m R□l R□h R□Uj R□&R□R□G□annirok,alikok,cpugnaihcdok□onik,gnik,7e remhk□gh+gh,akitrak□adannak,agn?
    k,9^asaliak,enotscak□tlu aj$aj□eciuj,i]lomoj,namrekoj□tsej,nosnej,Re zzaj,cpuenimsaj,d□esenapaj,tc?t^cc?t^xf,
    ruet□3t□2t□t□ruep□3p□2p□p□atop alooks^cpusir^C□□lavretn^etatsretn^egavonni□110{A&{atalosnocn^□Nd□Nd+N@wodahs 6&
```

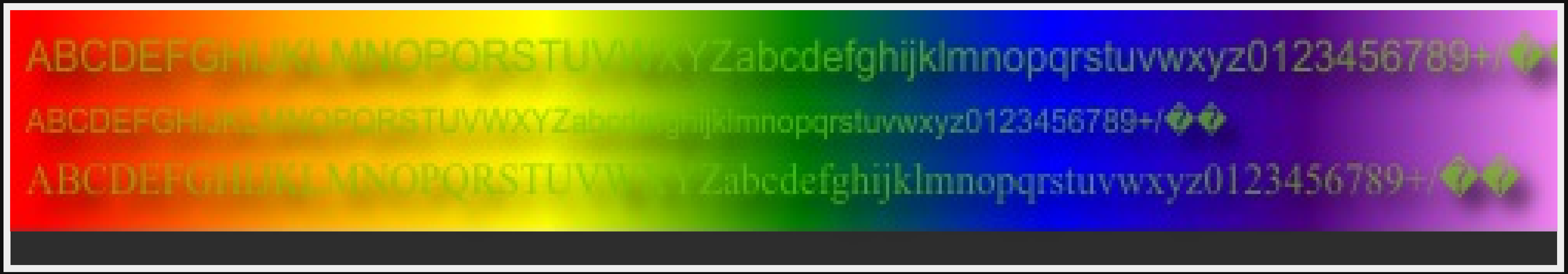
Fingerprint overview

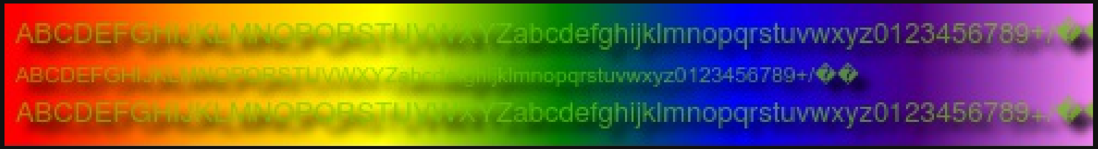
```
FP = {
        device: {
                browser : {
                        ...
                }, geoLocation : {
                        ...
                }, network : {
                        ...
                }, os : {
                        ...
                }
        }
}
```

Browser (1/2)

```
fingerprint : {
        audio : "25184b80d8388c1 ... 902ba5450536ee6b",
        plugin : "4efcd01f09577b ... 05a4a2cb4623e3e7",
        canvas : "21c639351f2978 ... 0998a381c173b101",
        font : "d7eaf0d8ac928e2d ... 5c89c7397db8c990",
        locale : "f097370e02e34c ... 2f3709051b051836",
        webGL : "16a36fb362eb4a7 ... 96ad2b04da5bcd08"
}
```

Zoom on canvas


ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/��
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/��
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/��


ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/�
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/��
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/�

Fonts enumeration (1/2)

- 836 fonts
- "Classical" technique, not canvas with canvas pixel precision
- Measure offsetWidth and offsetHeight

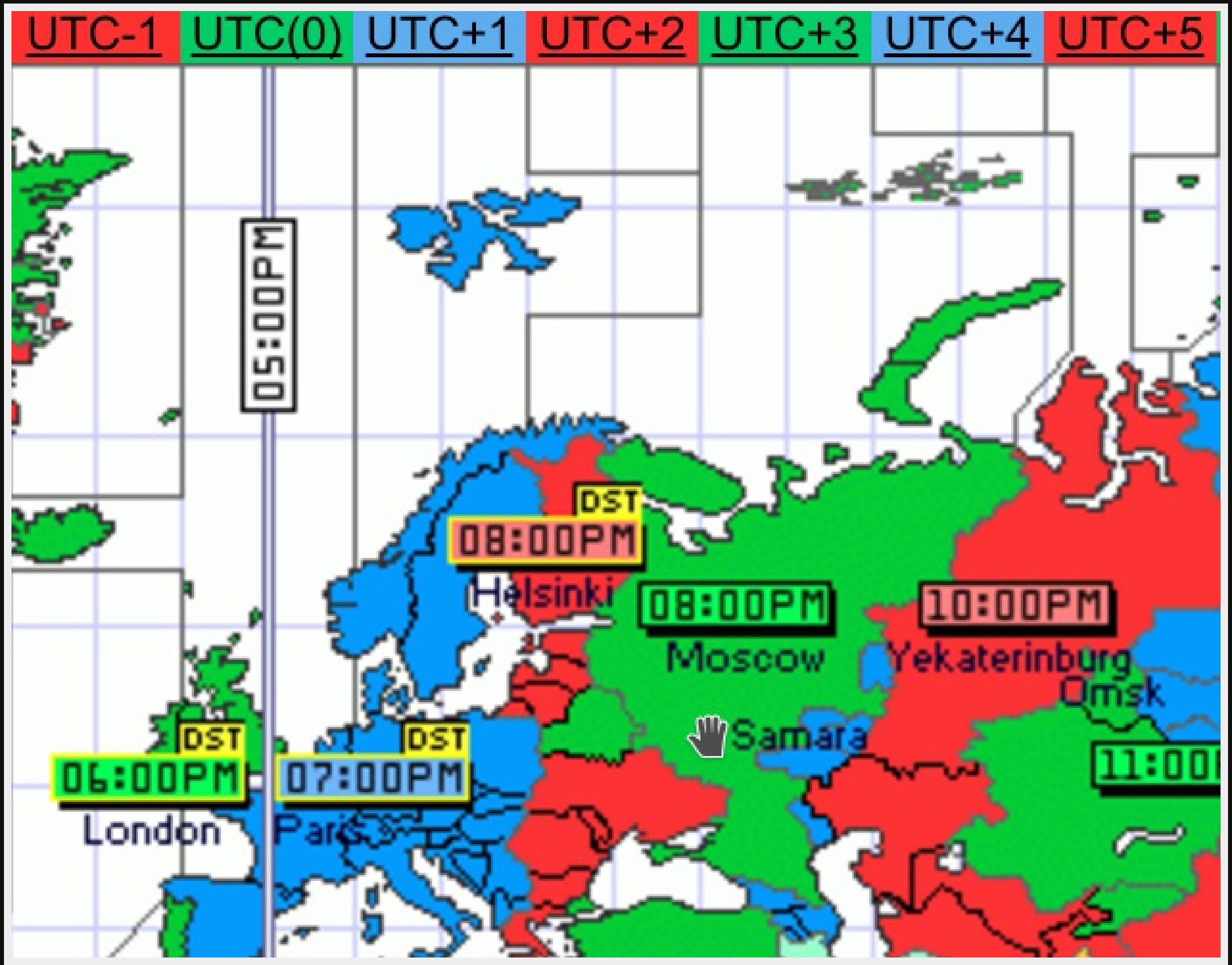
Fonts enumeration (2/2)

Example:

mmmmmmmmmmmmlli (621/80)

mmmmmmmmmmmmlli (793/102)

Locale (1/2)



UTC-1
UTC(0)
UTC+1
UTC+2
UTC+3
UTC+4
UTC+5
05:00PM
DST
08:00PM
Helsinki
08:00PM
Moscow
10:00PM
Yekaterinburg
Omsk
Samara
11:00
DST
06:00PM
London
DST
07:00PM
Paris

Locale (2/2)

```
var d = new Date;
var skip = d.getTimezoneOffset();
d.setTime(0);
var locale = "";
var ms = 0;
// 864E5 = number of ms in a day
for (;ms < 1769390779860;ms += 864E5) {
    d.setTime(ms);
    val = d.getTimezoneOffset();
    if (val !== skip) {
        locale += "" + val + Math.round(ms / 1E3);
        skip = val;
    }
}
```

WebGL

No 3D shapes rendering

- MAX_TEXTURE_MAX_ANISOTROPY_EXT
- WebGL version, renderer, vendor, antialias, vertex shaders best precision...

Browser (2/2)

```
is : {
        blockingAds : true,
        blockingCookies : false,
        spoofed : false,
        incognito false, // removed since v4
}
```

is.spoofed (1/2)

```
eval.toString().length
```

The output should be:

- 37 on Safari, Firefox
- 33 on Chrome
- 39 on Internet Explorer

Test existence of error.toSource() (only Firefox)

is.spoofed(2/2)

Check consistency between:

- OS extracted from UA
- navigator.oscpu
- navigator.platform

Check if device should have touch support

Private mode

On Firefox:

```
var request = window.indexedDB.open("mykey");

request.onerror = function(event) {
        if(event.target.error.name == "InvalidStateError") {
                console.log("Private mode");
        }
};
```

geoLocation

```
geolocation: {
        ISOCountryCode: "FR",
        city: "Fresnes-sur-Escaut",
        continent: "Europe",
        coordinates: "50.4338,3.5775",
        country: "France",
        postal: "59970",
        region: "Hauts-de-FRrance",
        is: {
                inTwoTimezones: false
        }
}
```

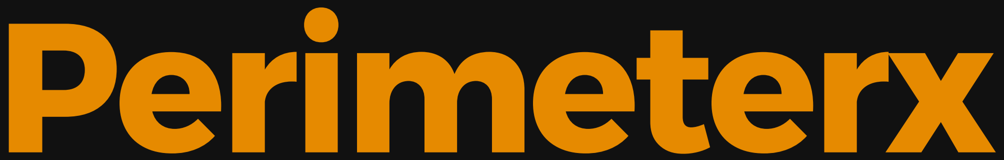
network.address

WebRTC, capable of detecting real IP address

```
network : {
        localAddress: 193. ...,
        publicAddress: 193. ...
}
```

OS

```
os: {
        batteryLevel: 0.91,,
        languages: "en,en-US,fr,fr-FR",
        name: "Linux",
        platform: "Linux x86_64",
        processors: 4,
        resolution: "1706x960x24x1706x960",
        screenDensity: "1.5",
        microphonesInstalled: 2,
        speakersInstalled: 2,
        webcamsInstalled: 1,
        touchScreenSupport: "0,true,false",
        videoCardDriver: "Google Inc. Google SwiftShader"
}
```


Perimeterx

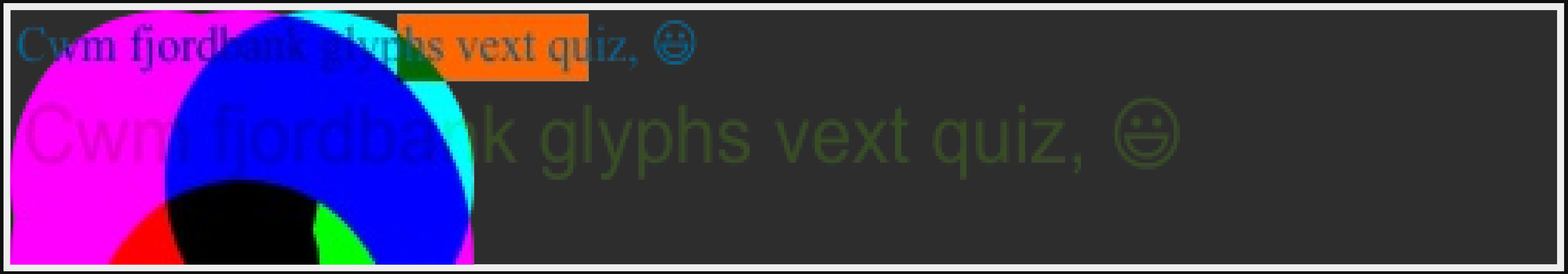
Script

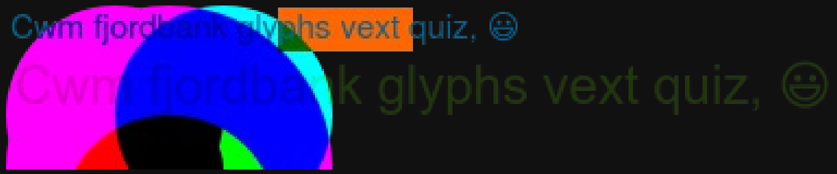
- Functions renamed
- Classical attributes
- More cautious about user's identity
- Catch all keyboard/mouse events
- Still makes use of Flash and ActiveXObject

Code sample

```
options.PX59 = error(model, "PX59", function() {
        return navigator.userAgent;
});
options.PX61 = error(model, "PX61", function() {
        return navigator.language;
});
options.PX63 = error(model, "PX63", function() {
        return navigator.platform;
});
```

Canvas


Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃


Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃

Fonts enumeration

- 65 fonts << 836 fonts
- offsetWidth/Height

WebGL (1/2)

```
self.PX276 = opts.canvasfp;
self.PX210 = opts.webglRenderer;
self.PX209 = opts.webglVendor;
self.PX277 = opts.webGLVersion;
self.PX278 = opts.shadingLangulageVersion;
self.PX279 = opts.unmaskedVendor;
self.PX280 = opts.unmaskedRenderer;
self.PX281 = opts.extensions;
self.PX282 = opts.webglParameters;
```

WebGL (2/2)

Simple shape rendering

Same code as Amiunique

- 95k+ fingerprints
- 5k+ ids
- 2000 distinct shapes

Detecting spoofers

Doesn't seem to be performed client side

Enough information to do it serverside

Specific features (1/2)

```
error(model, "PX190", function() {
        return window.chrome && (window.chrome.runtime &&
        window.chrome.runtime.id) || "";
});
```

Specific features (2/2)

```
navigator.sendBeacon;
navigator.msDoNotTrack; // IE only
document.documentMode; // IE only
document.location.ancestorOrigins; // Webkit only
```

Cautious

Check if plugins overwritten

```
return e = "function" == typeof navigator.plugins.toString ?
navigator.plugins.toString() : navigator.plugins.constructor &&
"function" == typeof navigator.plugins.constructor.toString ?
navigator.plugins.constructor.toString(): lr(navigator.plugins),
"[object PluginArray]" === e || "[object MSPluginsCollection]"
=== e || "[object HTMLPluginsCollection]" === e
```

Detecting web scrapers

```
window.callPhantom;
window.__nightmare;
...
window.__Selenium_IDE_Recorder;
```

Honeypot for scrapers

Add hidden links with no follow, only bots can see them since they are not rendered

```
function render(u, css) {
        var a = document.createElement("a");
        a.href = u;
        a.rel = "nofollow";
        a.appendChild(document.createTextNode("click"));
        if (css) {
        a.style.cssText = css;
        }
        a.target = "_blank";
        addEvent(a, "click", _init);
        document.head.appendChild(a);
}
```

Defense strategies

Fingerprinting may raise privacy issues

- Script blocking
- Don't be unique (decrease entropy)
- Break linkability (change)

Few countermeasures

- Ghostery
- Random Agent Spoofer (Extension)
- Brave (Browser)
- FPRandom (Modified browser)

More about fingerprinting

Amiunique project

Discover your fingerprint:

http://amiunique.org

Conclusion

Evolution since 2010 (Flash, new attributes)

Marketing vs security

Privacy issue