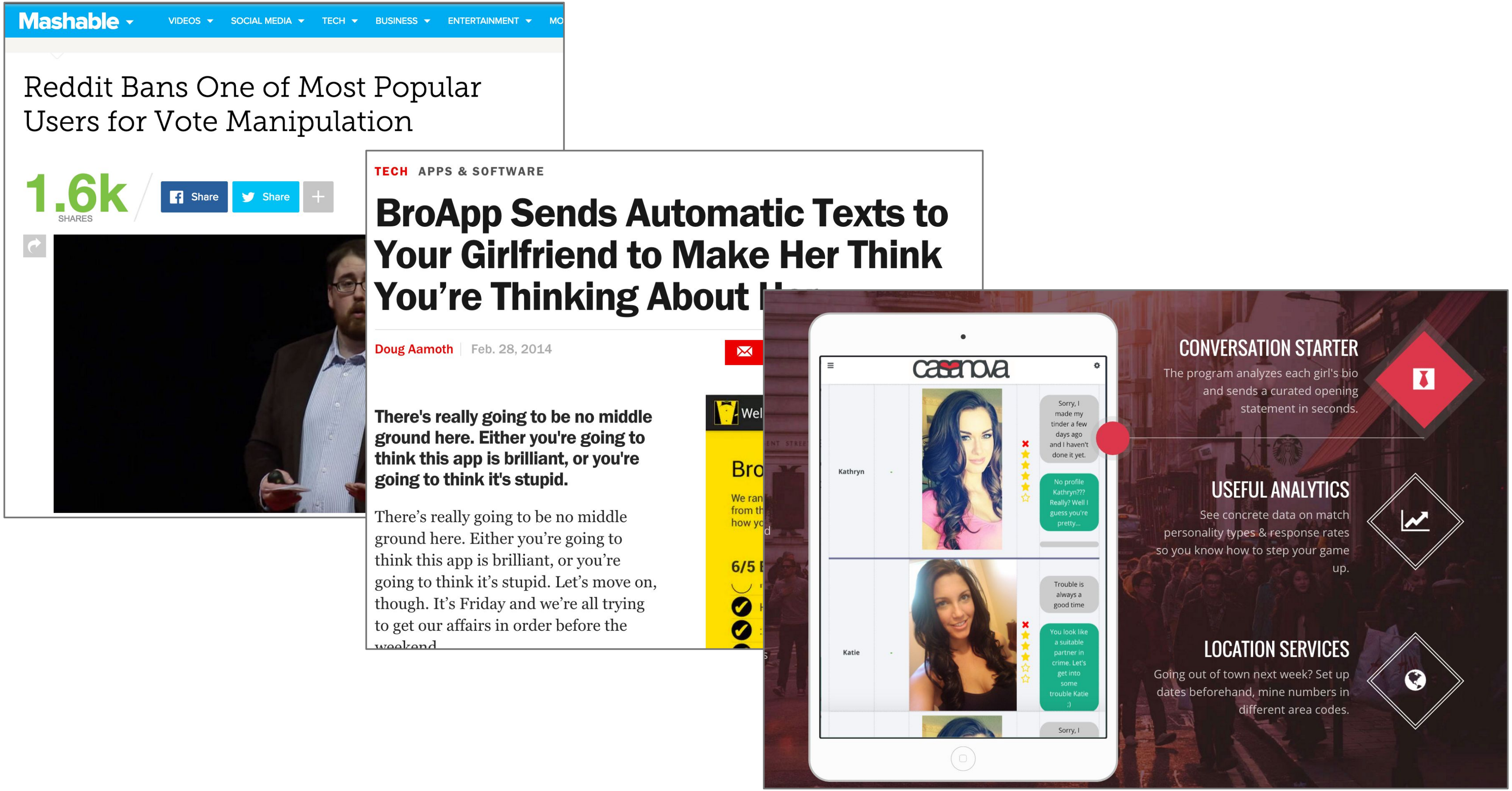
Picasso: Light-weight device class fingerprinting for web clients

Elie Bursztein, Artem Malyshev, Tadek Pietraszek, Kurt Thomas

Google Research



Reddit Bans One of Most Popular Users for Vote Manipulation

1.6k SHARES

TECH APPS & SOFTWARE

BroApp Sends Automatic Texts to Your Girlfriend to Make Her Think You're Thinking About H

Doug Aamoth | Feb. 28, 2014

There's really going to be no middle ground here. Either you're going to think this app is brilliant, or you're going to think it's stupid.

There's really going to be no middle ground here. Either you're going to think this app is brilliant, or you're going to think it's stupid. Let's move on, though. It's Friday and we're all trying to get our affairs in order before the weekend

Kathryn

Sorry, I made my tinder a few days ago and I haven't done it yet.

No profile Kathryn??? Really? Well I guess you're pretty...

Katie

Trouble is always a good time

You look like a suitable partner in crime. Let's get into some trouble Katie ;)

Sorry, I

CONVERSATION STARTER

The program analyzes each girl's bio and sends a curated opening statement in seconds.

USEFUL ANALYTICS

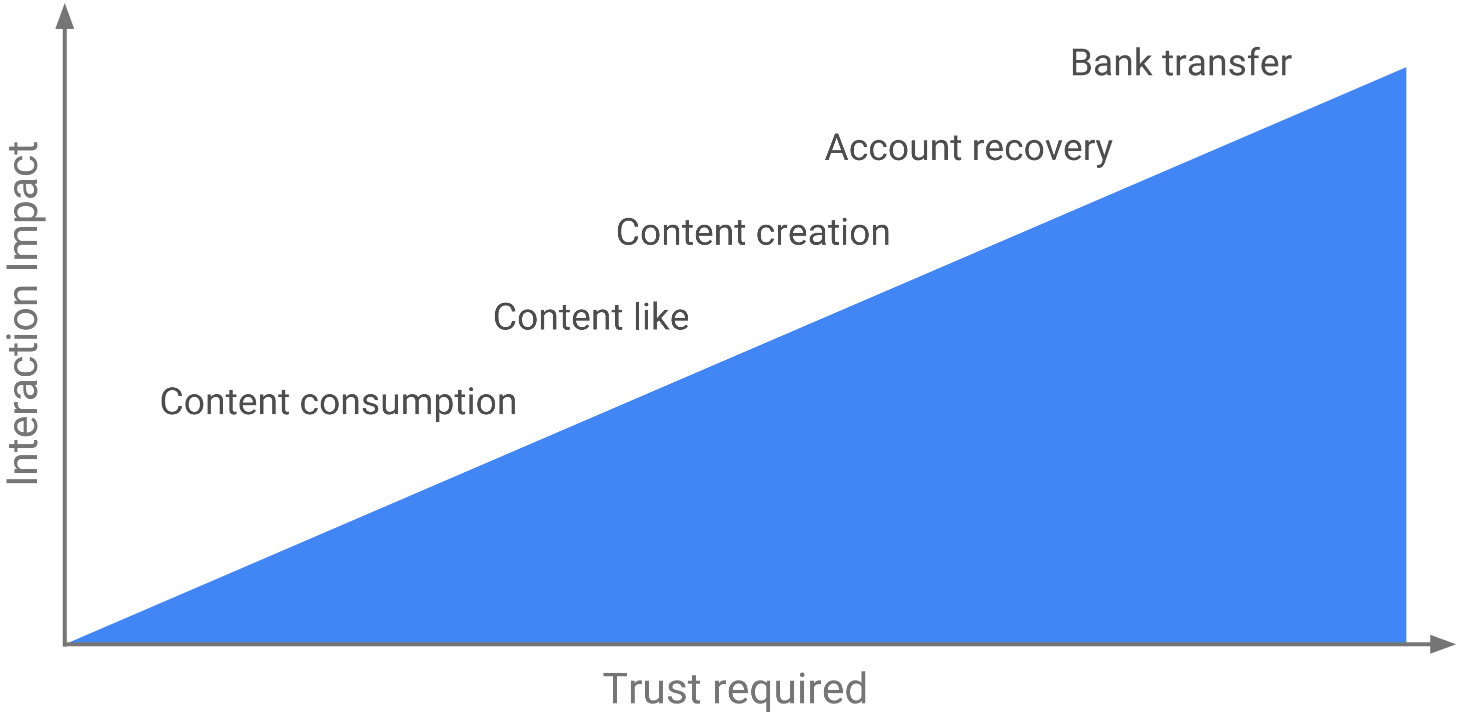
See concrete data on match personality types & response rates so you know how to step your game up.

LOCATION SERVICES

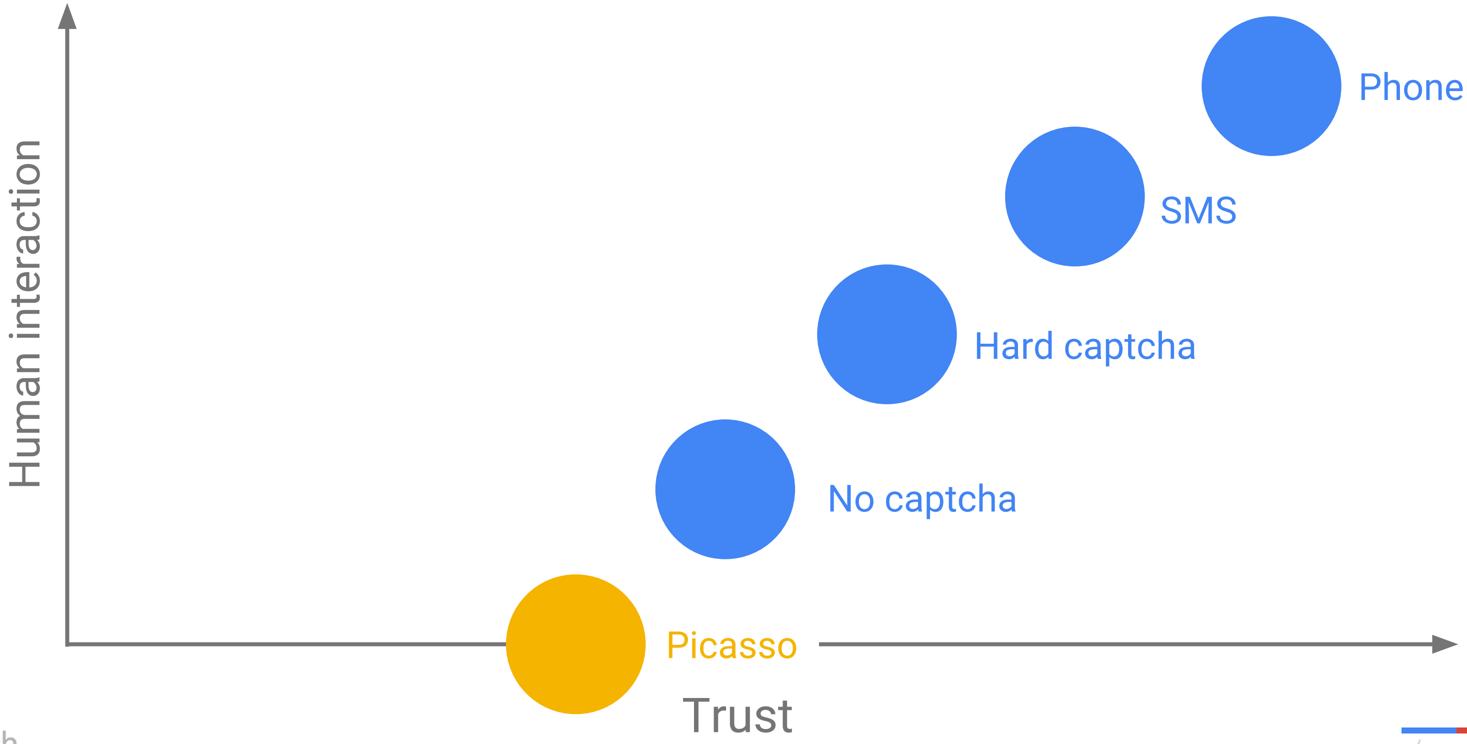
Going out of town next week? Set up dates beforehand, mine numbers in different area codes.

Keeping online interactions meaningful

Different interaction requires distinct level of trust



Verification methods trade-off



Goals

Remote device class attestation

Allow to enforce quotas and help anomaly detection

Proof of work

Enforce that attacker will expend 20ms of iOS time per request

Requirements

Cross-platform and cross-language

Any platform (Android, iOS) and any language (Javascript, SWIFT)

Accurate browsers and OS discrimination

Chrome OSX vs Safari OSX, Chrome Windows vs Chrome OSX

Emulators detection

Safari on iPhone vs Safari on an emulator

Constraints

No device modification

Must run on off-the-shelf devices

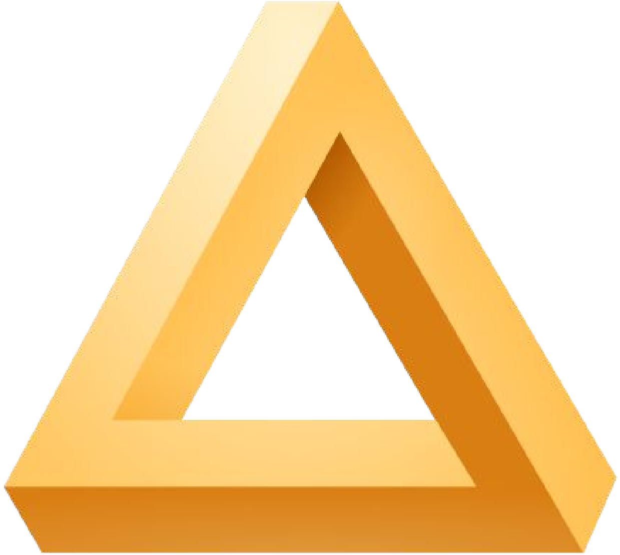
Fast and lightweight

Can be downloaded/executed often even on low-end devices

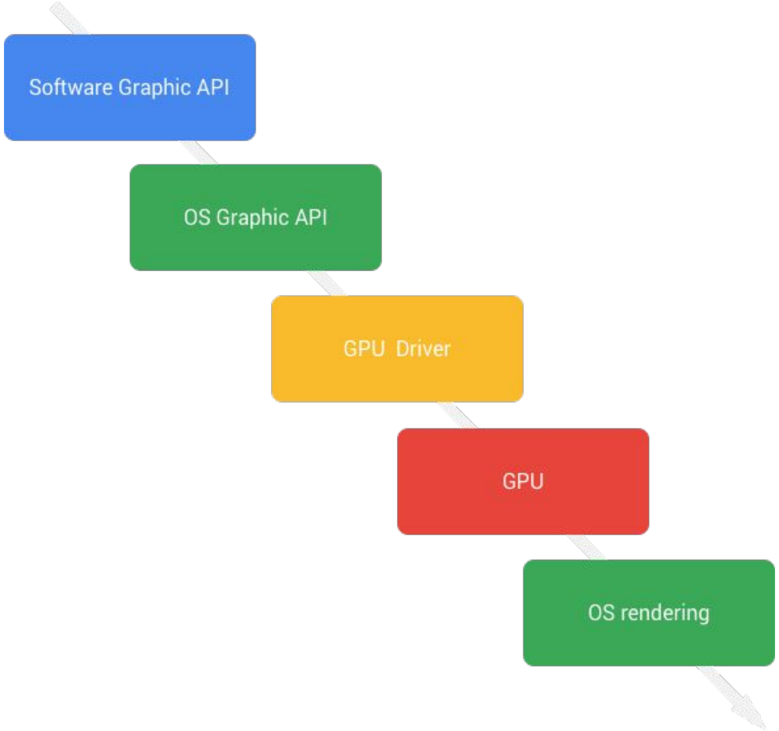
Tamper proof

Code to be shipped to clients and potentially executed offline

Mission Impossible?

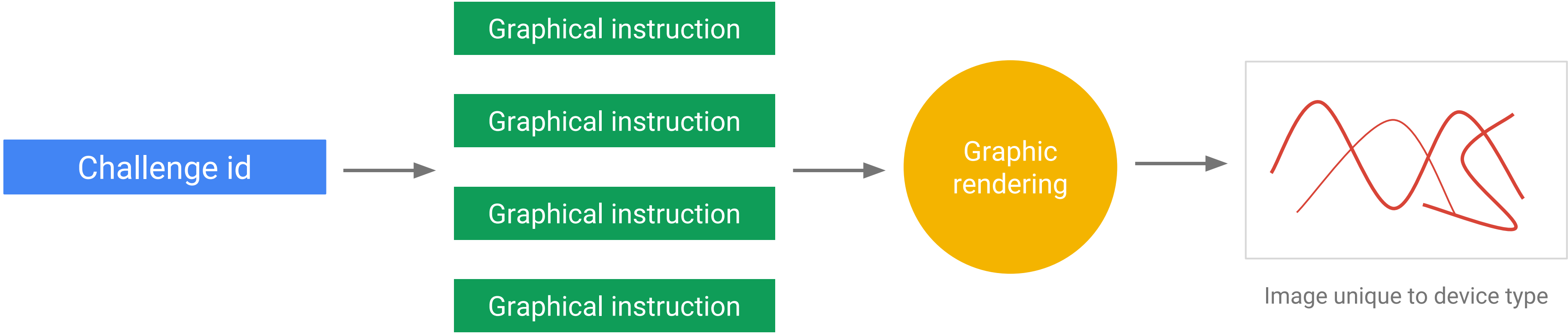


System overview



Use the graphical stack as a physically unclonable function

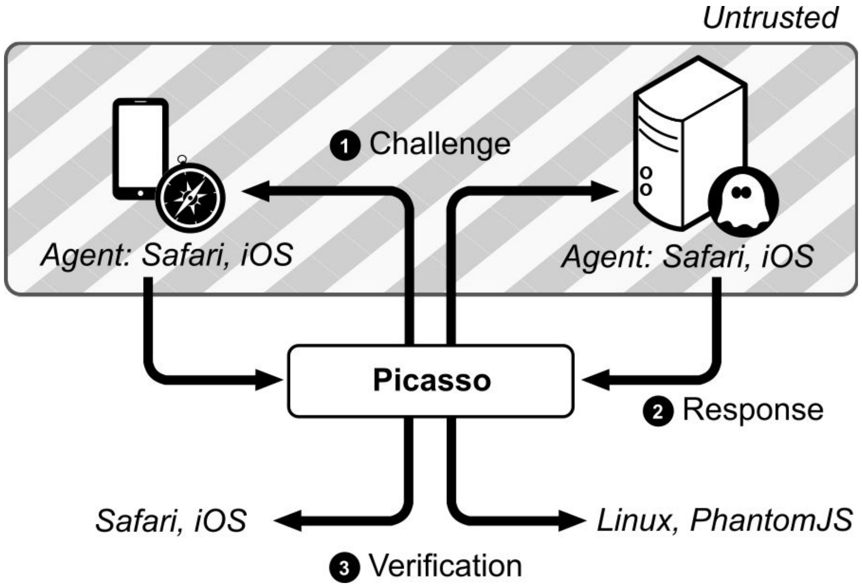
Principle


Challenge id
Graphical instruction
Graphical instruction
Graphical instruction
Graphical instruction
Graphic rendering
Image unique to device type

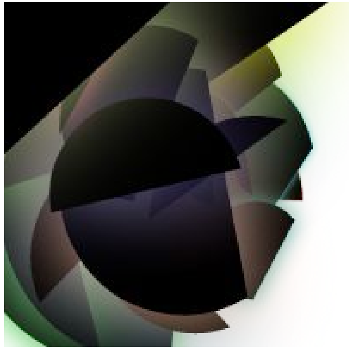
Graphical primitives used

- ⌒ Quadratic curve
- ∿ Bezier curve
- ○ Circle
- 𝓕 Font

Telling apart bots from devices

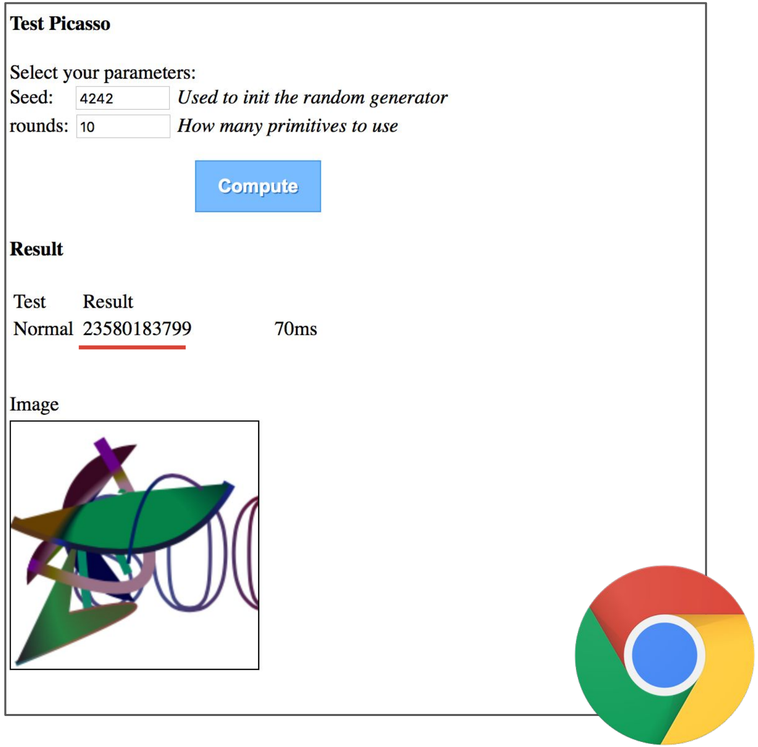


Why Picasso?



Evaluation

Demo



Test Picasso

Select your parameters:

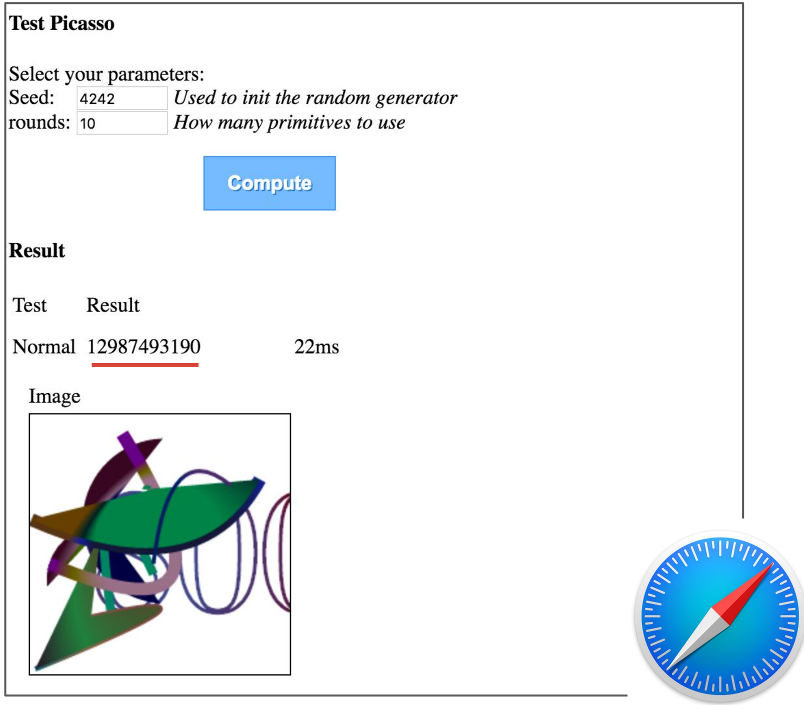
Seed: 4242 *Used to init the random generator*

rounds: 10 *How many primitives to use*

Result

Test	Result	
Normal	23580183799	70ms

Image



Test Picasso

Select your parameters:

Seed: 4242 *Used to init the random generator*

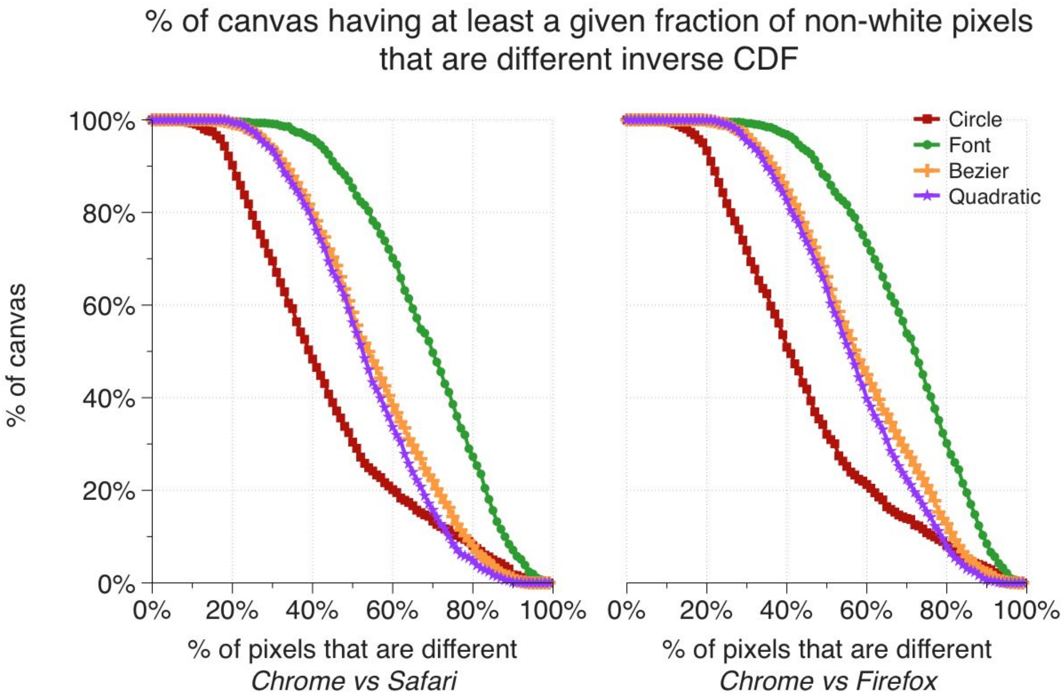
rounds: 10 *How many primitives to use*

Result

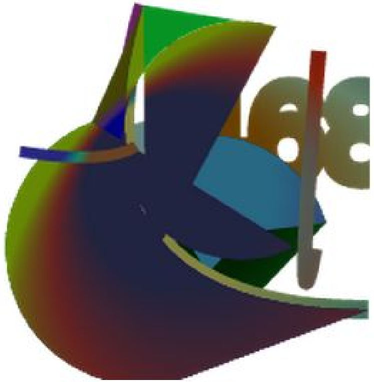
Test	Result	
Normal	12987493190	22ms

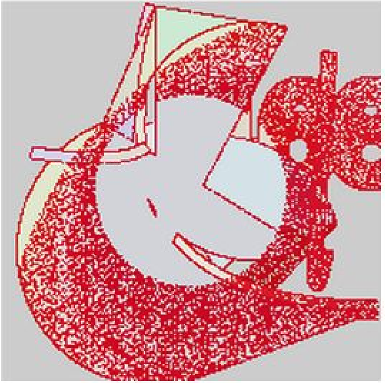
Image

Is the graphical stack really a PUF?

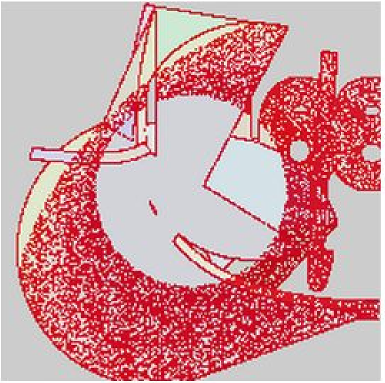


Browser difference heatmap

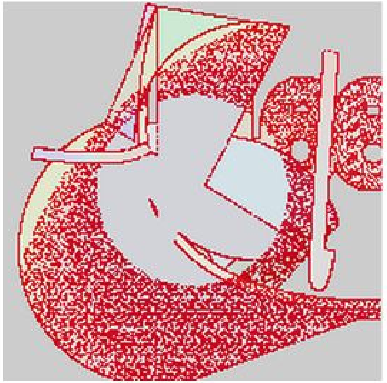




Chrome vs Firefox

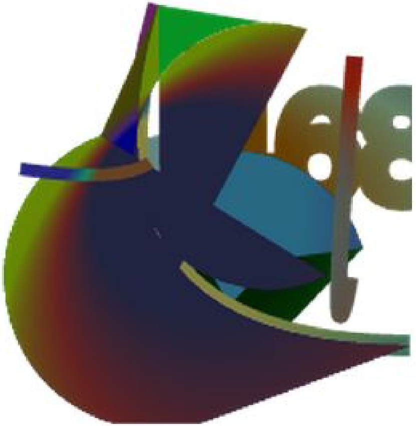


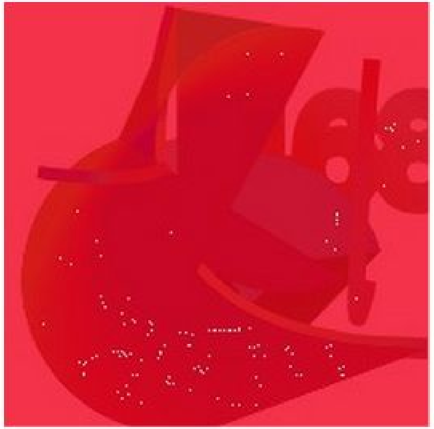
Chrome vs Safari



Firefox vs Safari

Safari on iPhone vs Safari on an emulator





Red imply pixels
are differents

Evaluation metrics

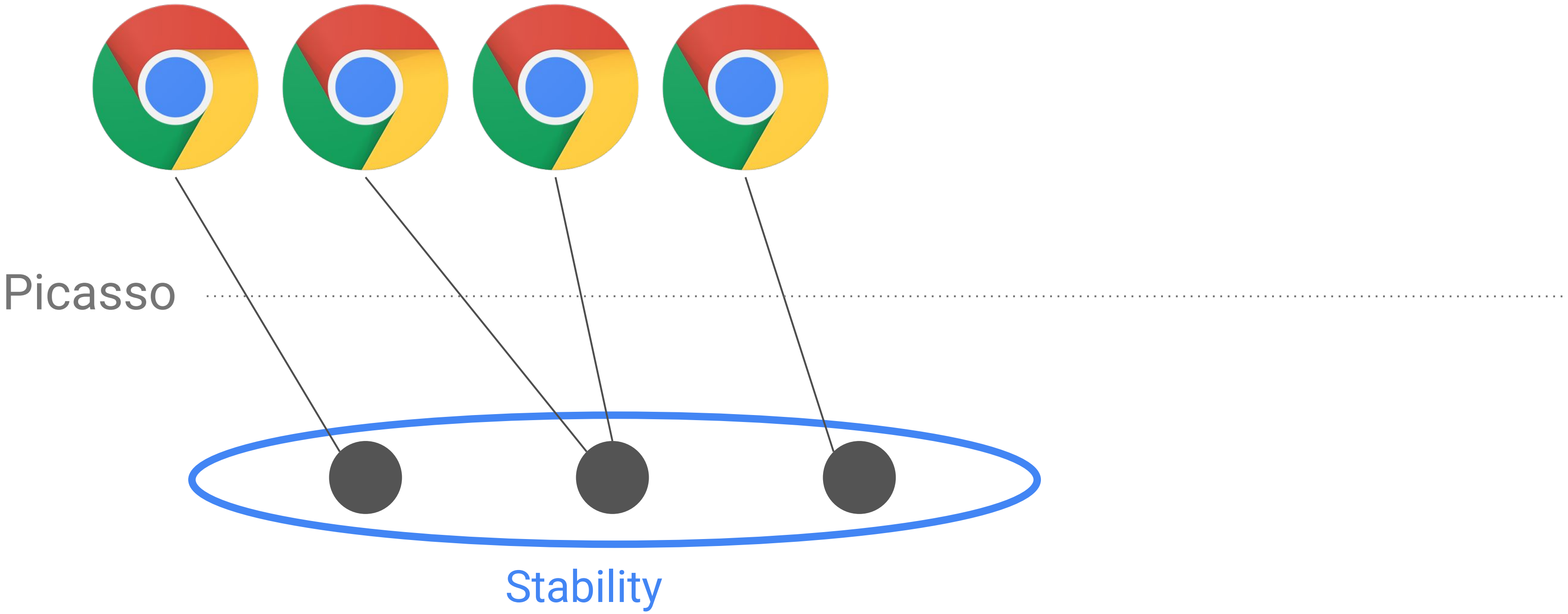
Uniqueness

Fraction of challenge response which are unique to a given device class

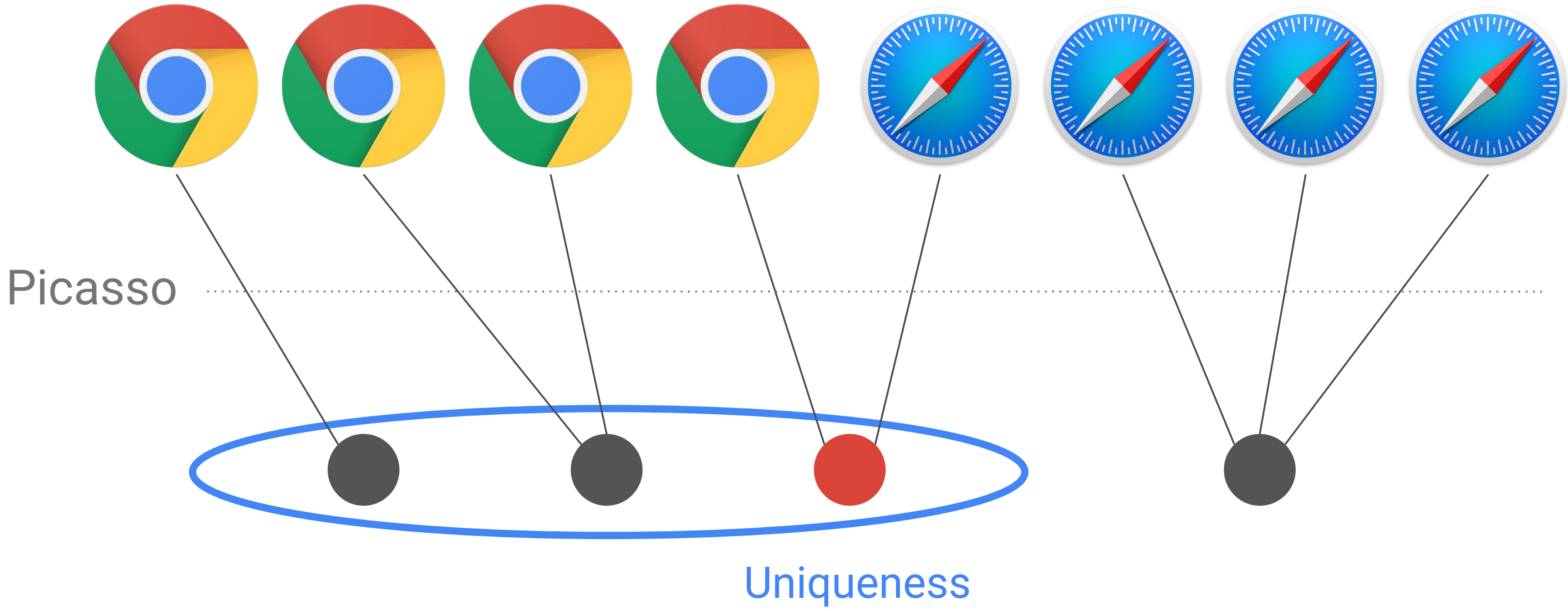
Stability

Number of distinct challenges response generated by a given class of device

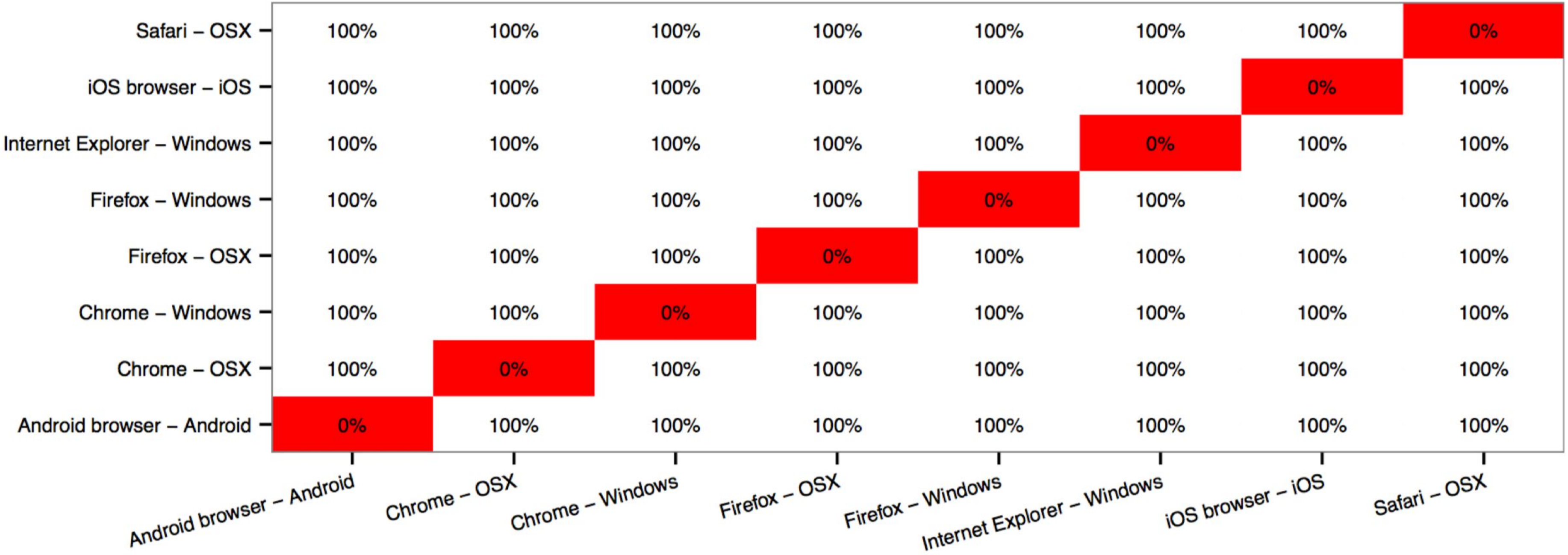
Stability illustrated



Uniqueness illustrated

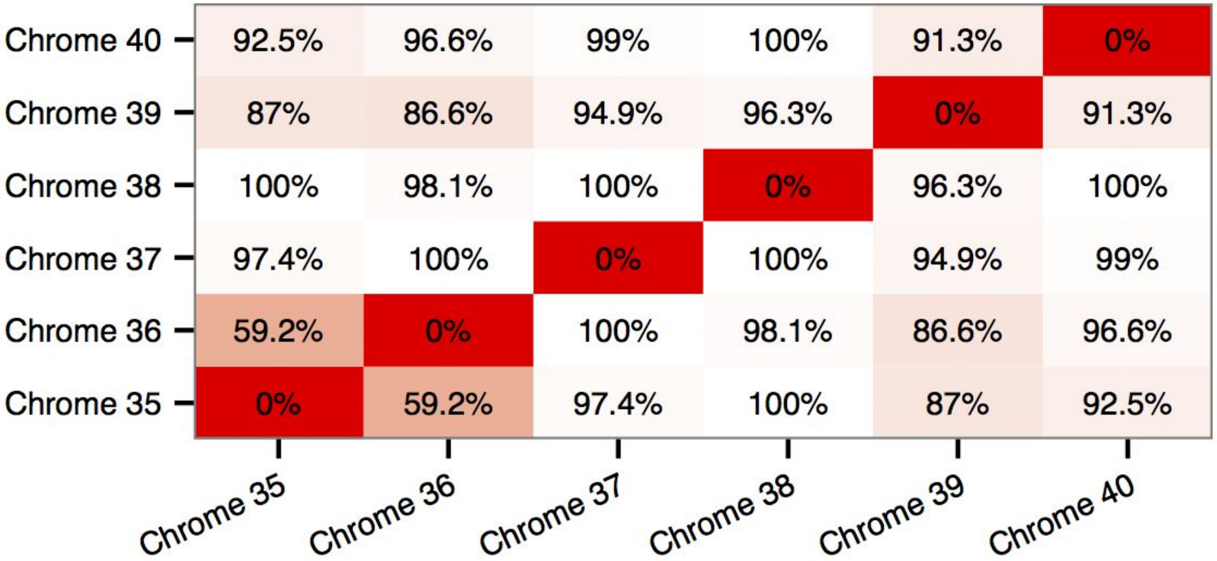


Uniqueness confusion matrix



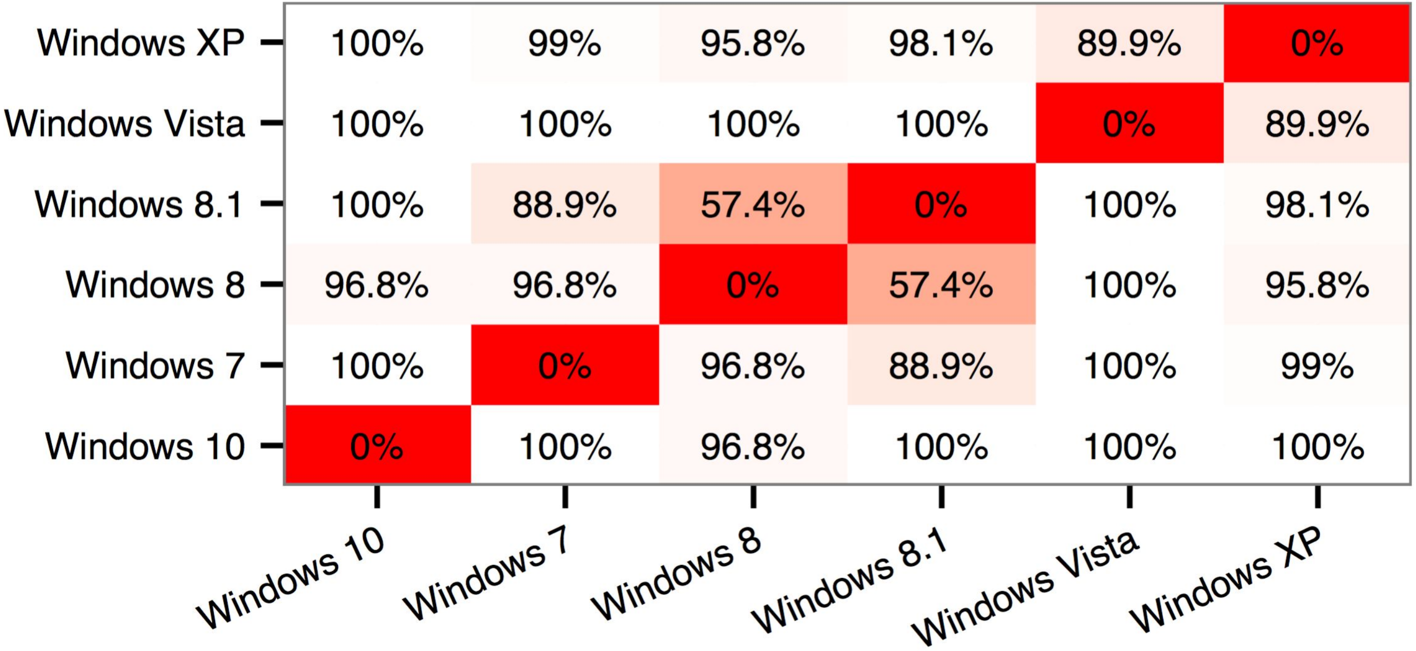
	Android browser – Android	Chrome – OSX	Chrome – Windows	Firefox – OSX	Firefox – Windows	Internet Explorer – Windows	iOS browser – iOS	Safari – OSX
Safari – OSX	100%	100%	100%	100%	100%	100%	100%	0%
iOS browser – iOS	100%	100%	100%	100%	100%	100%	0%	100%
Internet Explorer – Windows	100%	100%	100%	100%	100%	0%	100%	100%
Firefox – Windows	100%	100%	100%	100%	0%	100%	100%	100%
Firefox – OSX	100%	100%	100%	0%	100%	100%	100%	100%
Chrome – Windows	100%	100%	0%	100%	100%	100%	100%	100%
Chrome – OSX	100%	0%	100%	100%	100%	100%	100%	100%
Android browser – Android	0%	100%	100%	100%	100%	100%	100%	100%

Chrome uniqueness confusion matrix



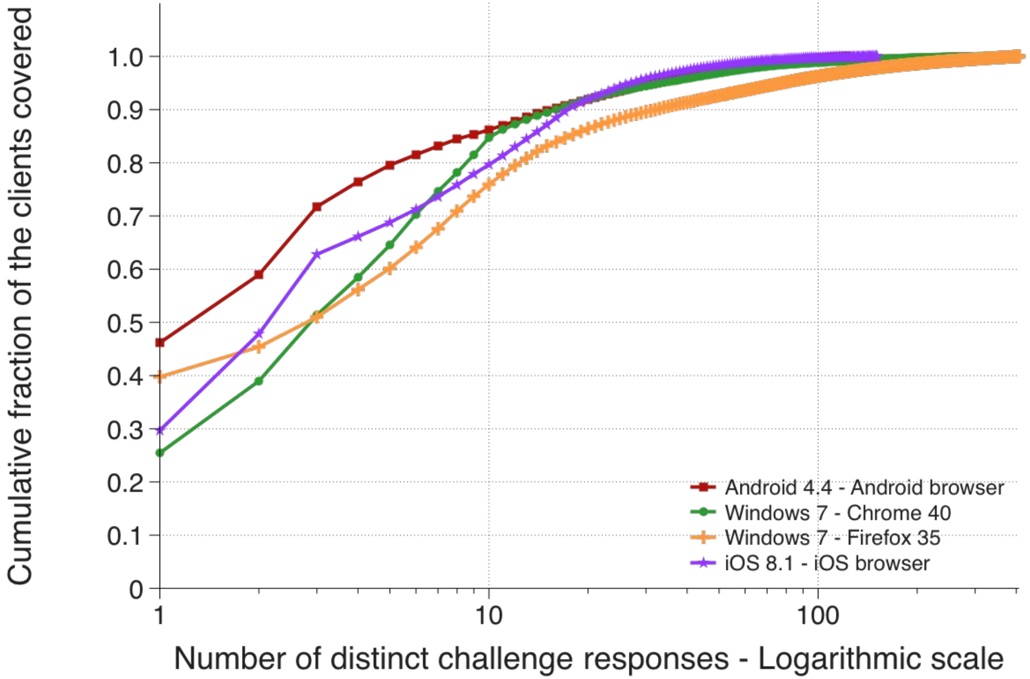
	Chrome 35	Chrome 36	Chrome 37	Chrome 38	Chrome 39	Chrome 40
Chrome 40	92.5%	96.6%	99%	100%	91.3%	0%
Chrome 39	87%	86.6%	94.9%	96.3%	0%	91.3%
Chrome 38	100%	98.1%	100%	0%	96.3%	100%
Chrome 37	97.4%	100%	0%	100%	94.9%	99%
Chrome 36	59.2%	0%	100%	98.1%	86.6%	96.6%
Chrome 35	0%	59.2%	97.4%	100%	87%	92.5%

Windows uniqueness confusion matrix



	Windows 10	Windows 7	Windows 8	Windows 8.1	Windows Vista	Windows XP
Windows XP	100%	99%	95.8%	98.1%	89.9%	0%
Windows Vista	100%	100%	100%	100%	0%	89.9%
Windows 8.1	100%	88.9%	57.4%	0%	100%	98.1%
Windows 8	96.8%	96.8%	0%	57.4%	100%	95.8%
Windows 7	100%	0%	96.8%	88.9%	100%	99%
Windows 10	0%	100%	96.8%	100%	100%	100%

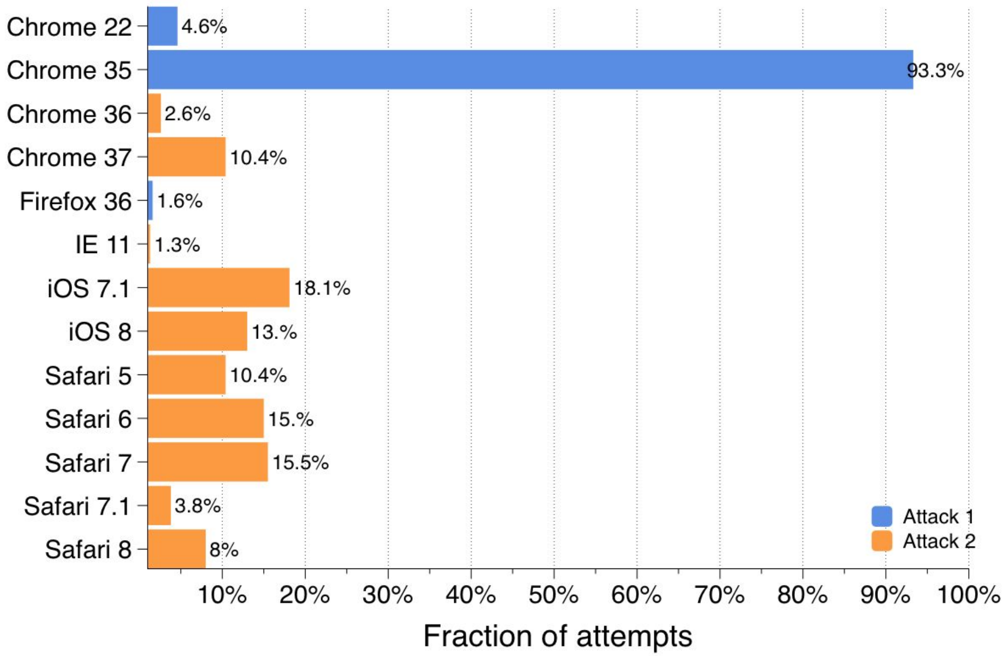
Stability



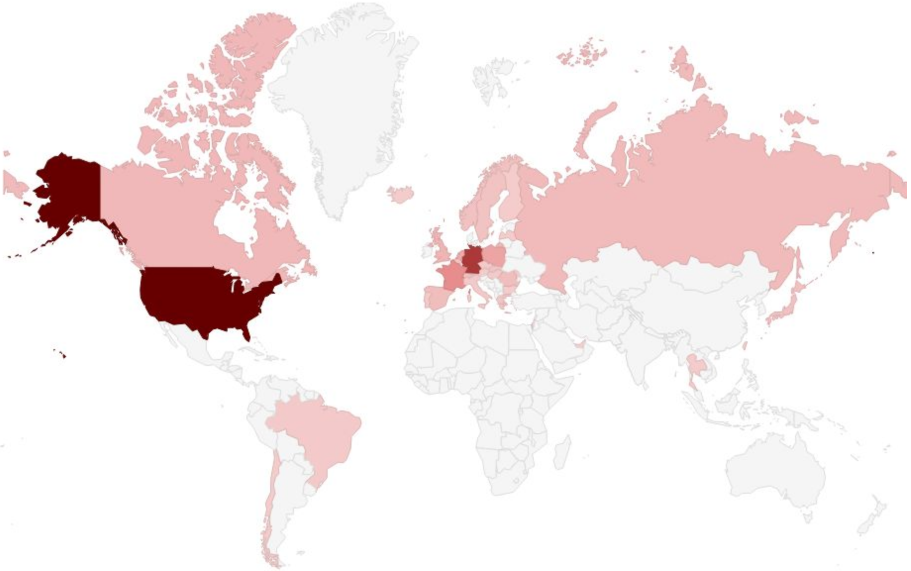
Cumulative fraction of the clients covered
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1
10
100
Number of distinct challenge responses - Logarithmic scale
Android 4.4 - Android browser
Windows 7 - Chrome 40
Windows 7 - Firefox 35
iOS 8.1 - iOS browser

War story

Brute-force attempts from EC2 via proxies



Proxies geo-distribution



Thanks

g.co/research/protect