Exercise Session VI: Anonymous Communication Systems

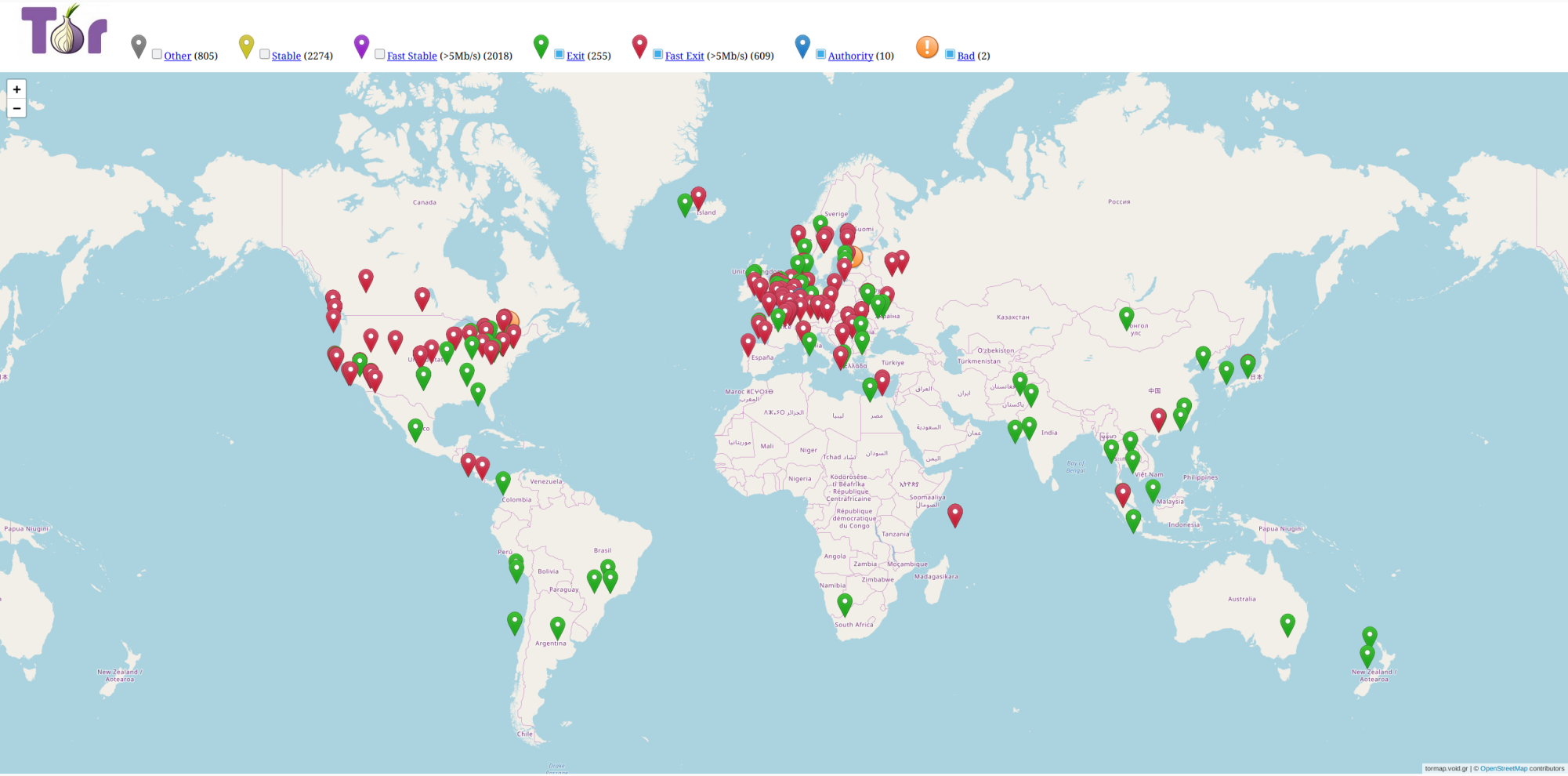
Network Security

Matteo Scarlata

29/10/2020

ETH Zurich

Context

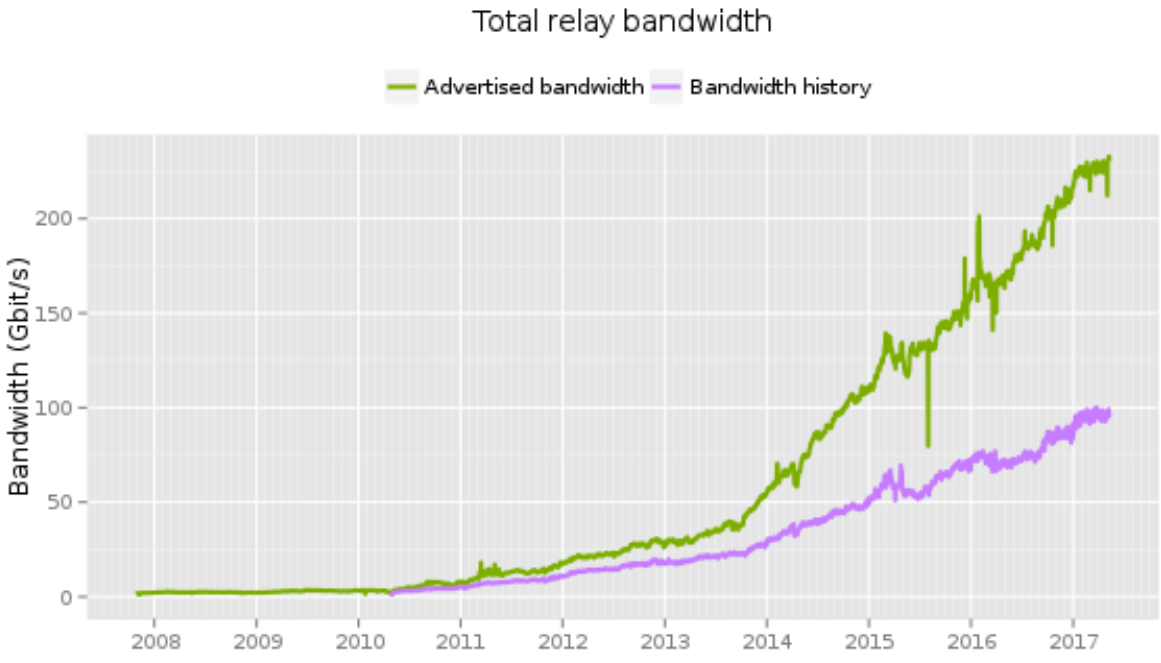


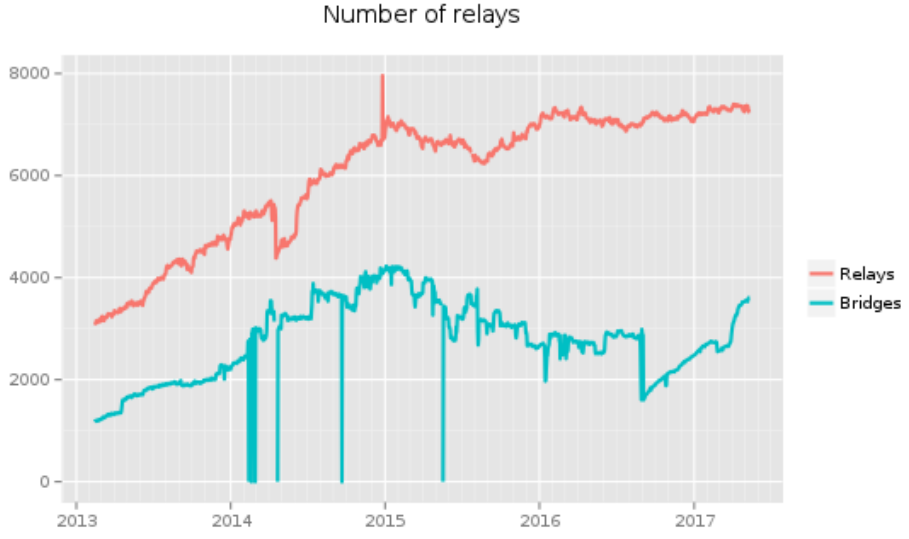
tormap.void.gr

- Slides from George Danezis, University College London

Tor wins!

- Today:
  - Over 7000 relays.
  - Over 200 Gbit/s.
  - About 2M users.
  - About 1 sec latency (median).
  - Tor Project $2M/y
- Hidden Services.
- Censorship:
  - Bridges.
  - Hidden Transports.
  - Open problems.





The Tor Project - https://metrics.torproject.org/

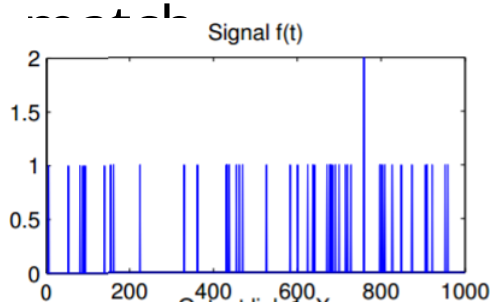
Why tor won the 2000s-2010s?

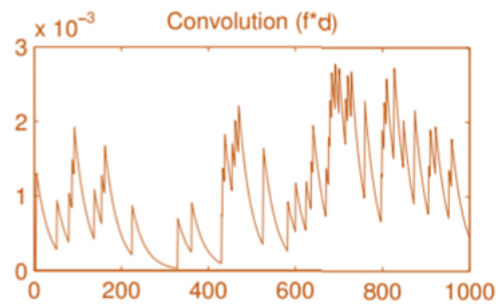
- Killer app: the web & TCP abstraction.
  - SOCKS Proxy -> Tor Browser bundle.
  - Email, lists on the decline, plagued by abuse and spam.
  - Hidden (web) Services.
- Interactivity & Usability:
  - Low(er) RTT does not require complex error correction / repetition.
  - Use TCP as substrate – failed connections detected immediately.
  - Can use for email + IM too.
  - "Anonymity loves company!"
- Low latency & cost:
  - Pre-open circuits to minimize crypto overhead.
  - 1-10 seconds (tor) vs. 30-60 mins (mixminion)
  - How? Do not protect against global adversary.

Mix networks have problems: can mixes they really protect against GPA?

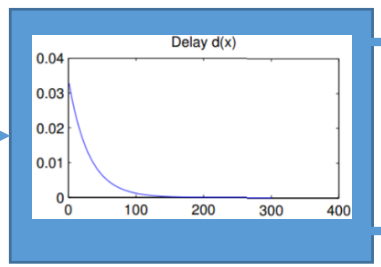
Tor problems: Stream Tracing attacks

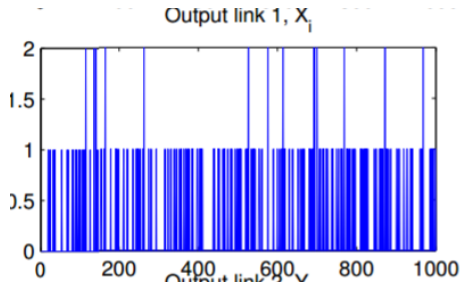
- An adversary can link two points of an anonymous circuit.
- How? Make a model template of output from input, and match

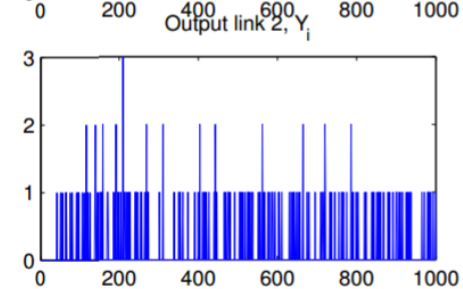




Tor Router with delay

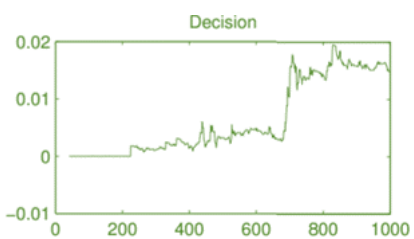






Template: distribution of outputs

Decision:



George Danezis: The Traffic Analysis of Continuous-Time Mixes. Privacy Enhancing Technologies 2004: 35-50

And many more problems …

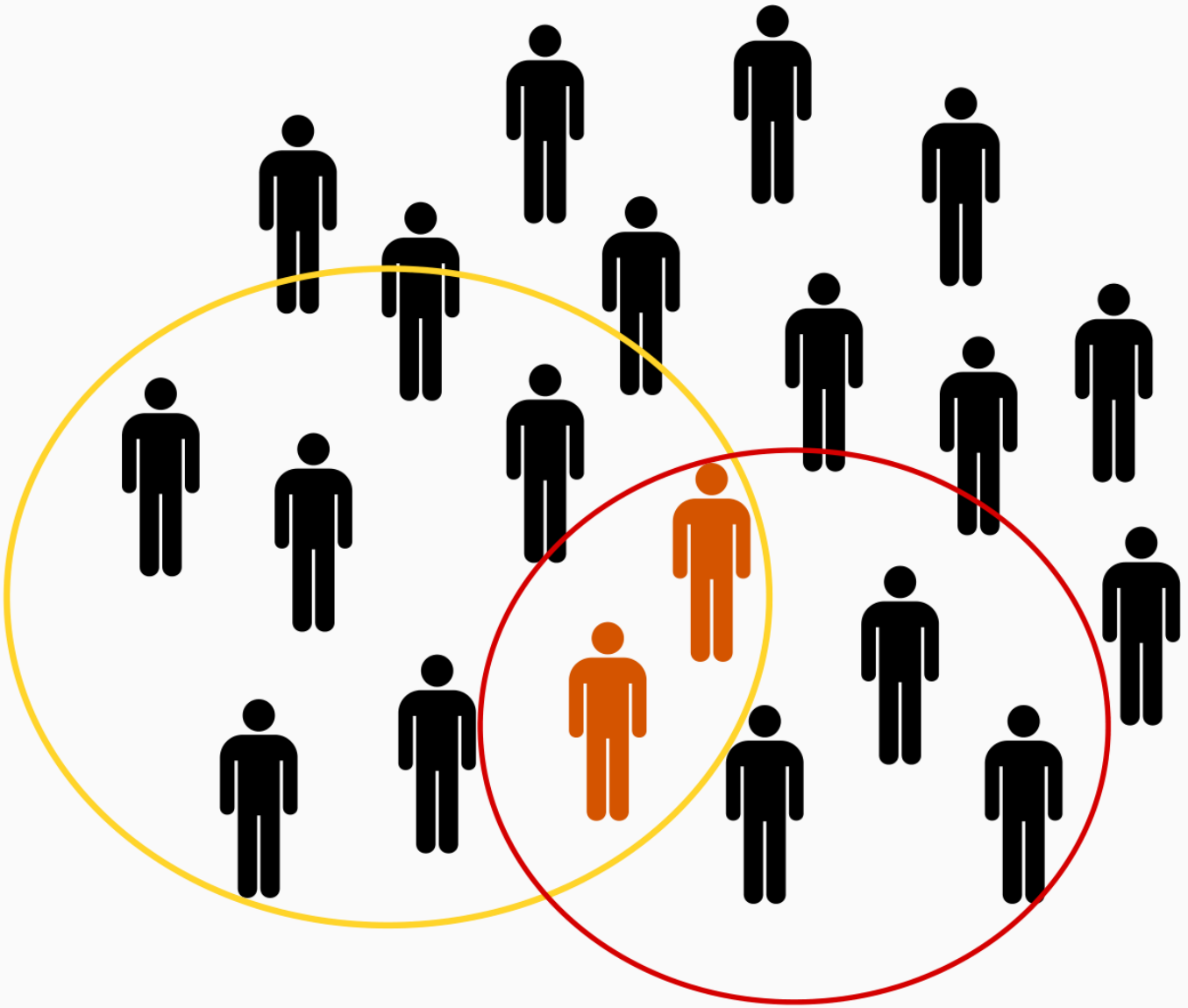
- Traffic analysis:
  - Sampling attacks
  - IX, AS sampling & BGP rerouting attacks
  - +Many mix attacks: DoS & epistemic attacks (do not matter because no GPA.)

- Tor is both too much and too little:
  - Too little: real adversaries can gain near GPA capabilities, or enough to break Tor. The Snowden revelations confirm this.
  - Too much: if it is trivial to link two points simpler design is possible:
    (1) No need for multiple layers of encryption.
    (2) A single hop security is all you get after a long time.

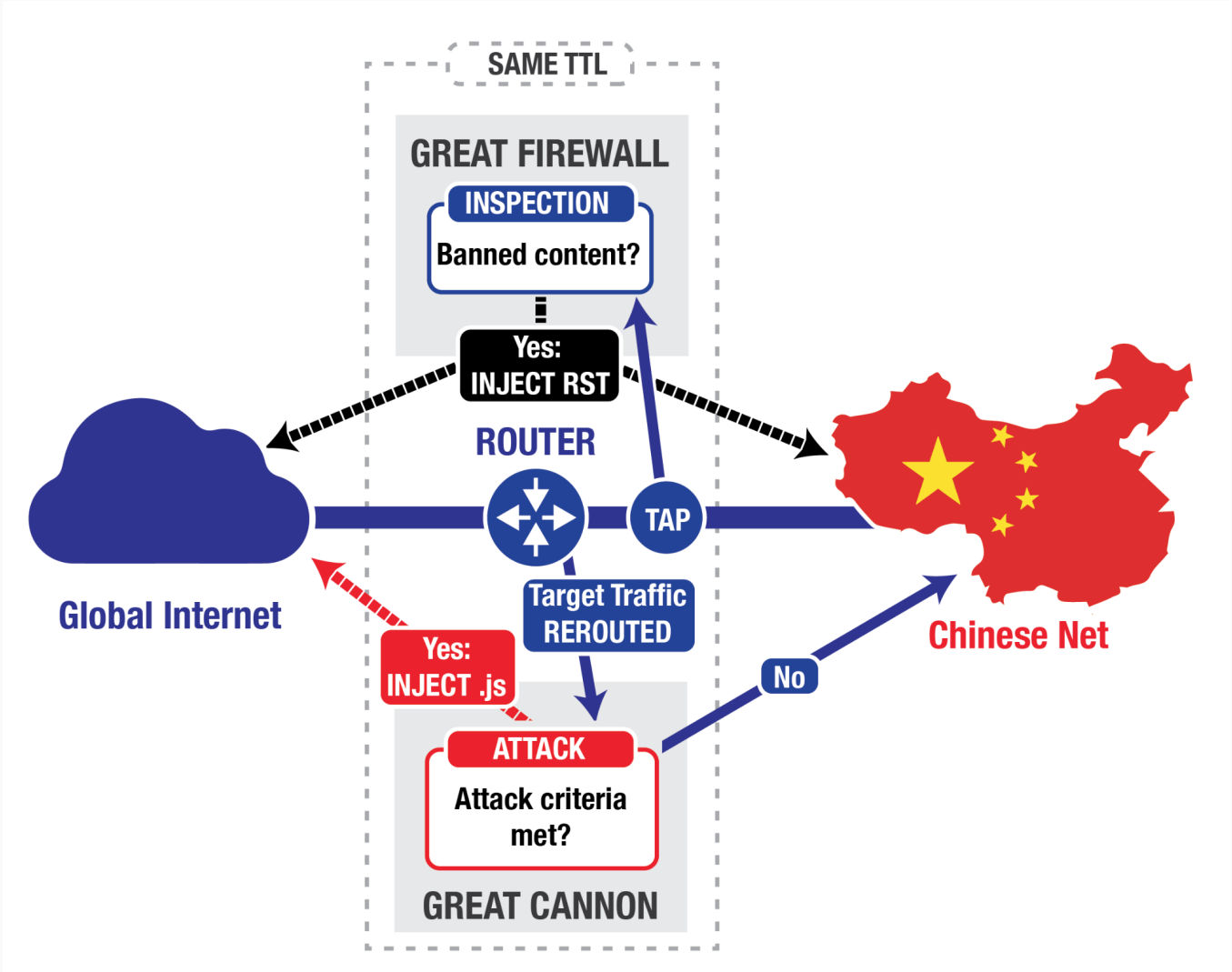
In conclusion: Tor is great if you want to hide from a relatively weak adversary. Not so great against more powerful adversaries…

Exercises

Small anonymity Set

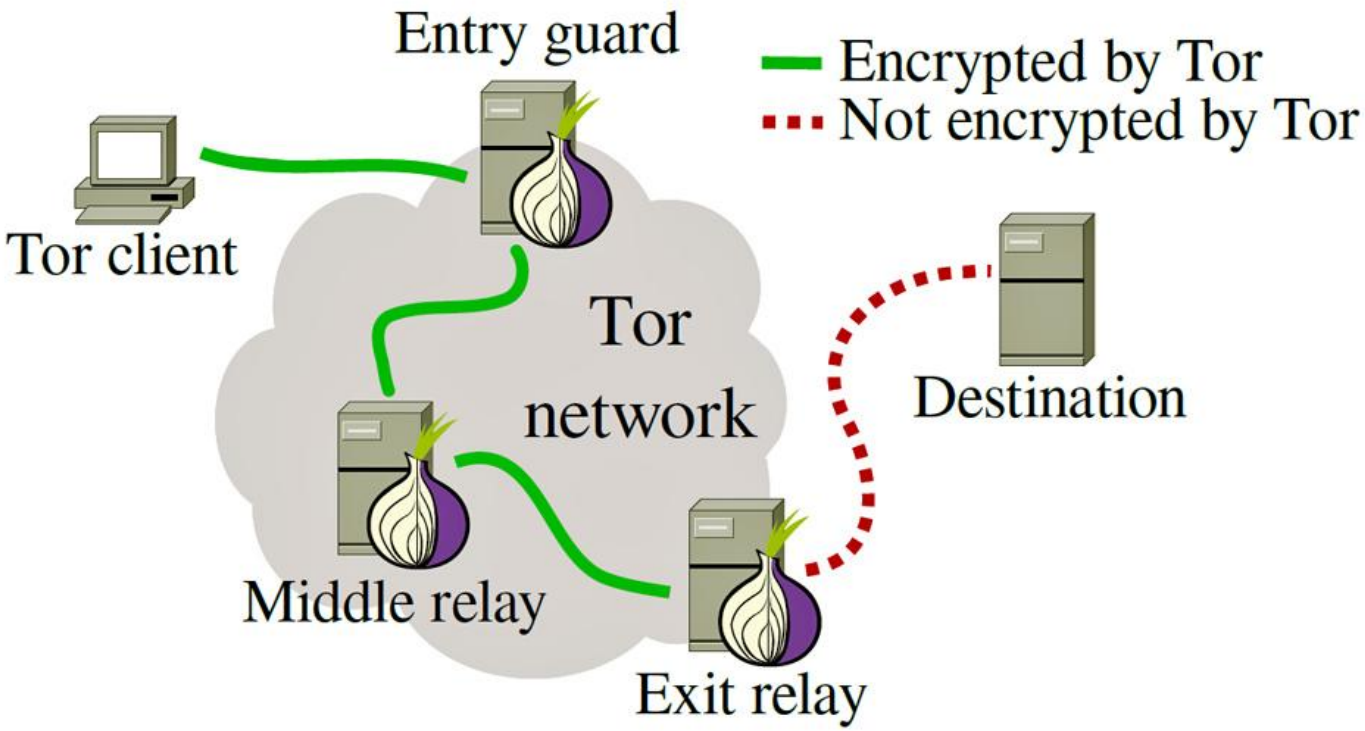


Censorship

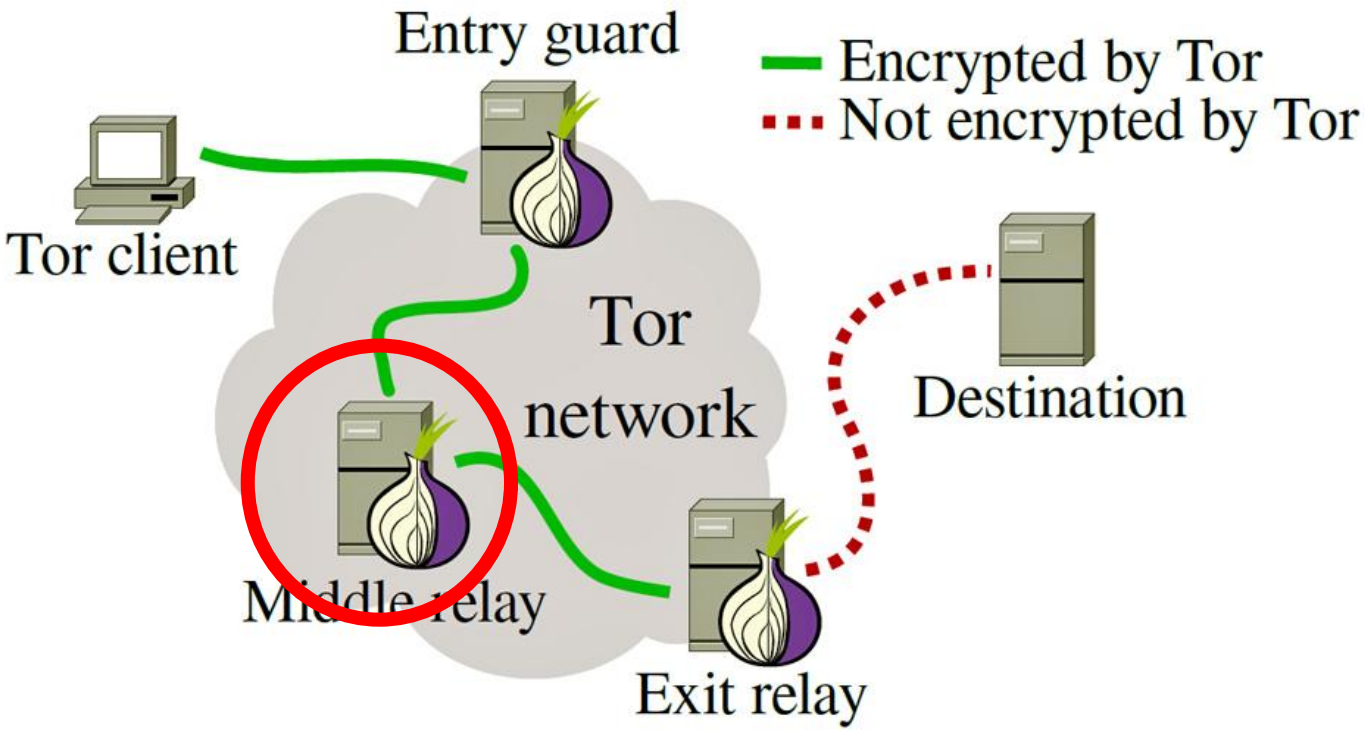


https://citizenlab.ca/2015/04/chinas-great-cannon/

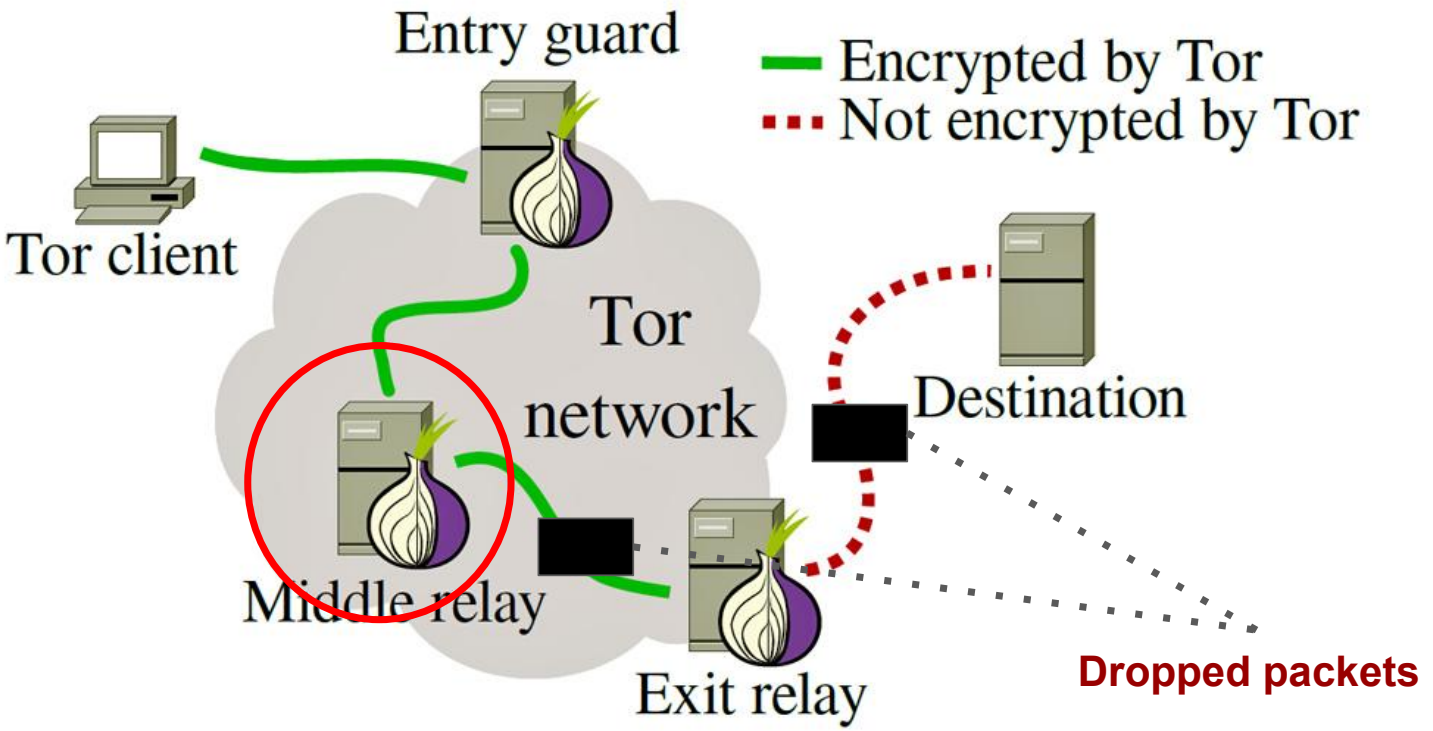
Statistical Attacks



Statistical Attacks



Statistical Attacks



Office attacks

- CVE-2017-11882: RCE via equation editor

Office attacks

- CVE-2017-11882: RCE via equation editor
- CVE-2018-0802: RCE via buffer overflow

Office attacks

- CVE-2017-11882: RCE via equation editor
- CVE-2018-0802: RCE via buffer overflow
- CVE-2017-0199: RCE via visual basic macro

Office attacks

- CVE-2017-11882: RCE via equation editor
- CVE-2018-0802: RCE via buffer overflow
- CVE-2017-0199: RCE via visual basic macro
- CVE-2019-1035: RCE via buffer overflow

But you said pdf!

But you said pdf!

50 CVEs in 50 Days: Fuzzing Adobe Reader

December 12, 2018

Research By: Yoav Alon, Netanel Ben-Simon

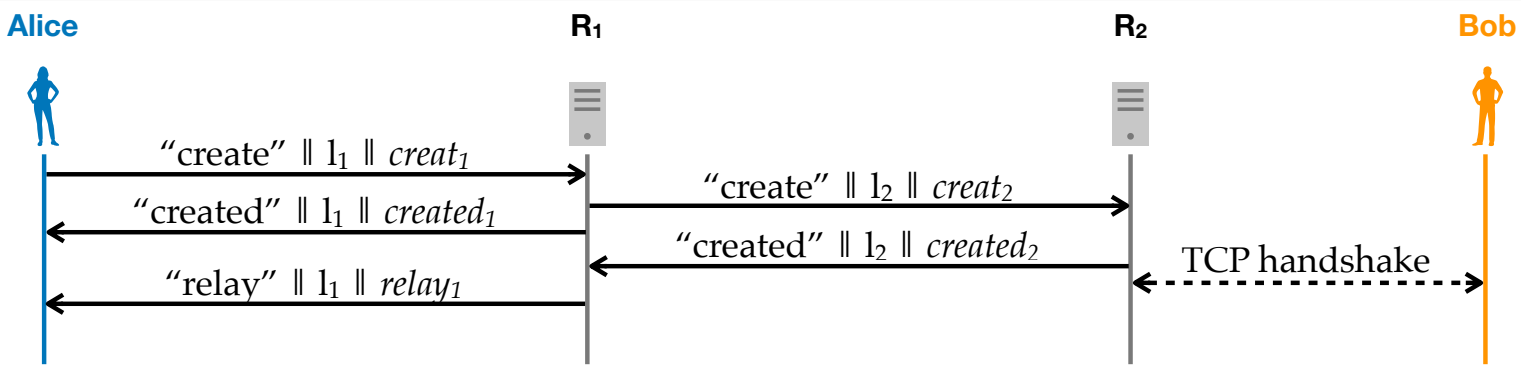
But you said pdf!

JavaScript for Acrobat - Adobe Inc.

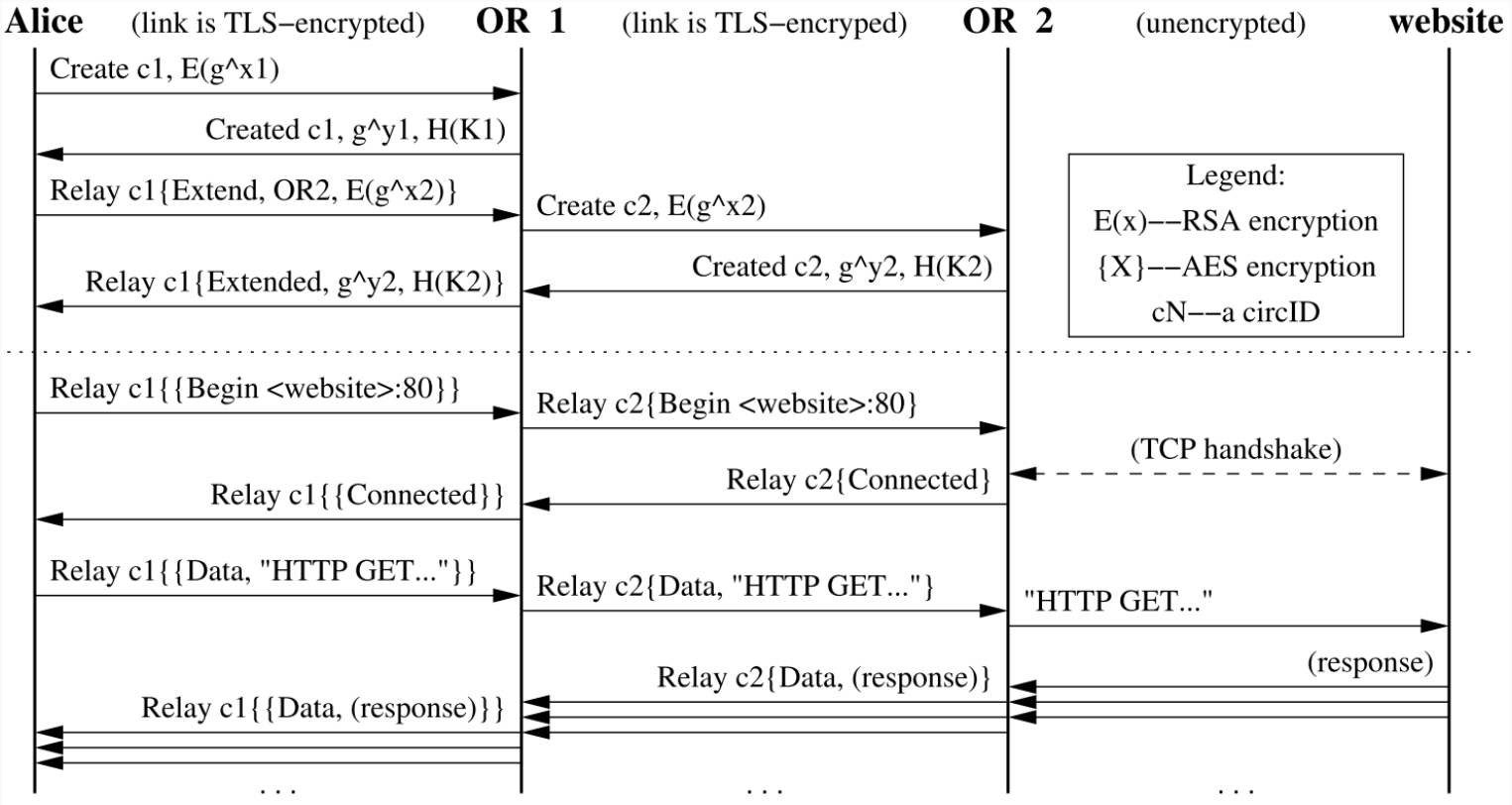
https://www.adobe.com/devnet/acrobat/javascript.html

Based on **JavaScript** version 1.5 of ISO-16262 (formerly known as ECMAScript), **JavaScript** in Adobe Acrobat software implements objects, methods, and properties that enable you to manipulate **PDF** files, produce database-driven **PDF** files, modify the appearance of **PDF** files, and much more.

New setup


Alice
R1
R2
Bob
"create" ‖ l1 ‖ creat1
"created" ‖ l1 ‖ created1
"relay" ‖ l1 ‖ relay1
"create" ‖ l2 ‖ creat2
"created" ‖ l2 ‖ created2
TCP handshake

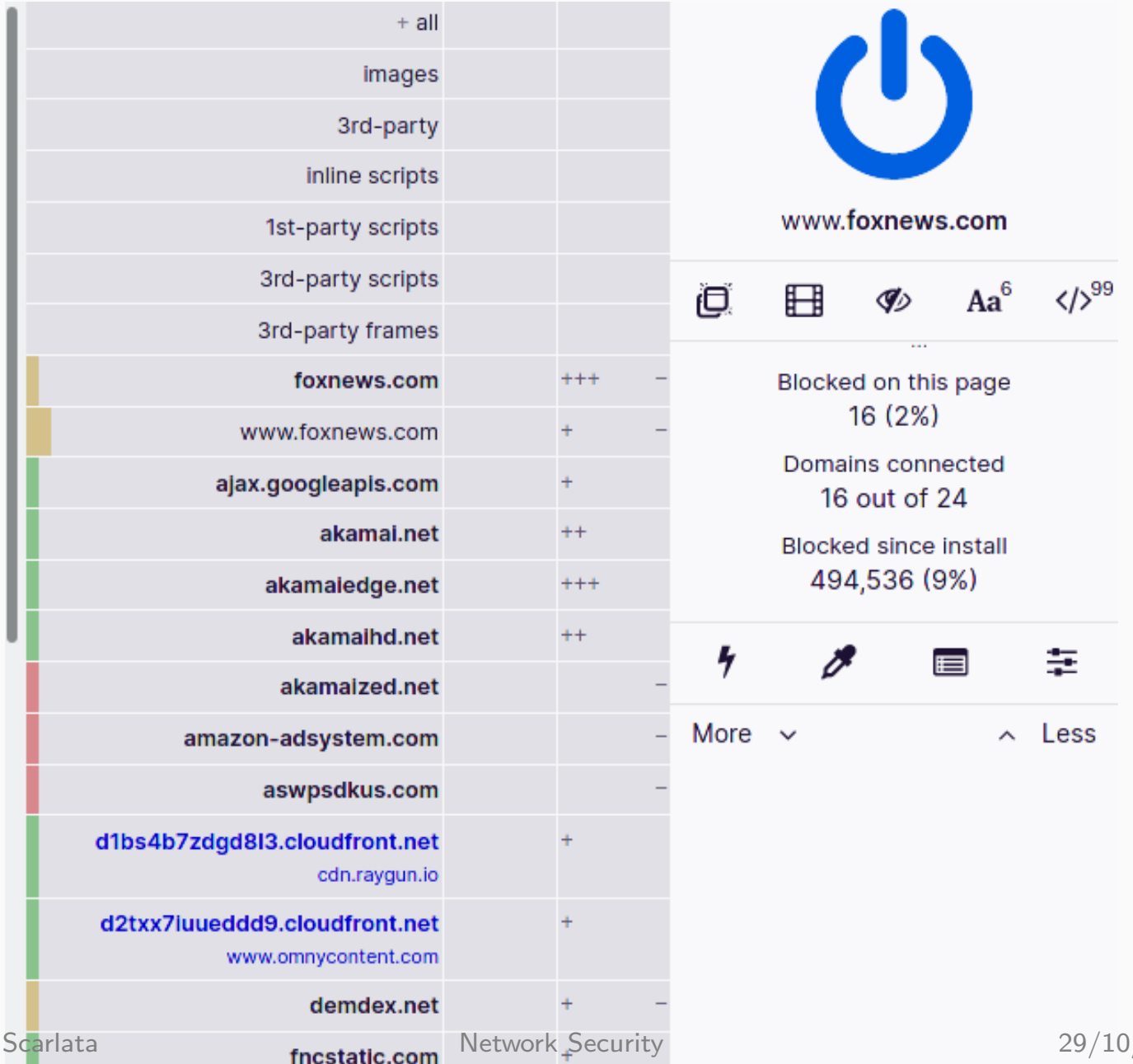
Traditional setup



Internet Dog

Image from The New Yorker cartoon by Peter Steiner, 1993.

Cookies


+ all
images
3rd-party
inline scripts
1st-party scripts
3rd-party scripts
3rd-party frames
foxnews.com +++ –
www.foxnews.com + –
ajax.googleapis.com +
akamai.net ++
akamaiedge.net +++
akamaihd.net ++
akamaized.net –
amazon-adsystem.com –
aswpsdkus.com –
d1bs4b7zdgd8l3.cloudfront.net
cdn.raygun.io +
d2txx7luueddd9.cloudfront.net
www.omnycontent.com +
demdex.net + –
fncstatic.com +
www.foxnews.com
Aa6
</>99
Blocked on this page
16 (2%)
Domains connected
16 out of 24
Blocked since install
494,536 (9%)
More
Less

Cookies


Crewmate
There are 2 Impostors among us
15
demdex.net
c.amazon-ad system.com
foxnews.com
google-analytics.com
js-agent.newrelic.com

Browser Fingerprinting

Browser Fingerprinting

the User agent header
the Accept header
the Connection header
the Encoding header
the Language header
the Upgrade Insecure Requests header
the Referer header
the Cache-Control header
the BuildId of the browser
the list of plugins
the platform

Browser Fingerprinting

the cookies preferences (allowed or not)

the Do Not Track preferences

the timezone

the screen resolution and its color depth

the use of local storage

the use of session storage

a picture rendered with the HTML Canvas element

a picture rendered with WebGL

Supported Audio formats

Supported Video formats

the presence of AdBlock

the list of fonts

Browser Fingerprinting: I'm not unique!

My browser fingerprint

Are you unique ?

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users

All time : 6.74%
30 days : 4.24%

All time : 41.30%
30 days : 47.13%

Version 82

All time : 0.08%
30 days : 1.54%

No JS

All time : 12.19%
30 days : 27.85%

Browser Fingerprinting

How is the fingerprint collected?

Browser fingerprints are also called cookieless monsters because it is not necessary to install any form of cookie t
and transparent for the user. Any third-party interested in fingerprinting can exploit a set of different techniques t

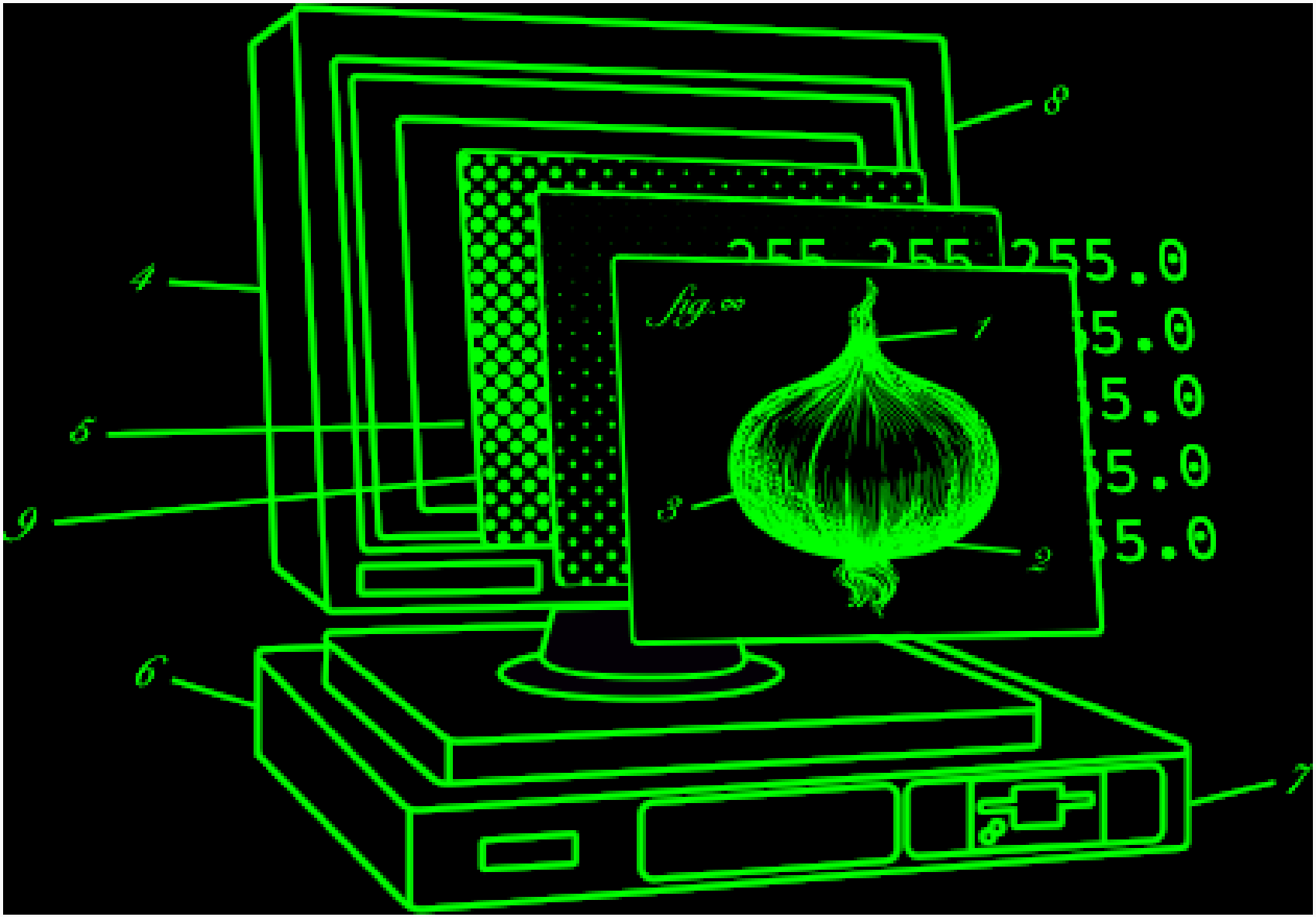
- the user agent and the accept headers are automatically sent to websites when a connection is initiated.
- JavaScript gives access to many browser-populated features like the plugins installed on the user's device.
- If the Flash plugin is installed, its rich programming interface (API) provides access to many system-specific
- Through the display of an HTML5 Canvas element, it is possible to collect small differences in the hardware between devices. The smallest pixel difference can be detected. This is called canvas fingerprinting.

Browser Fingerprinting

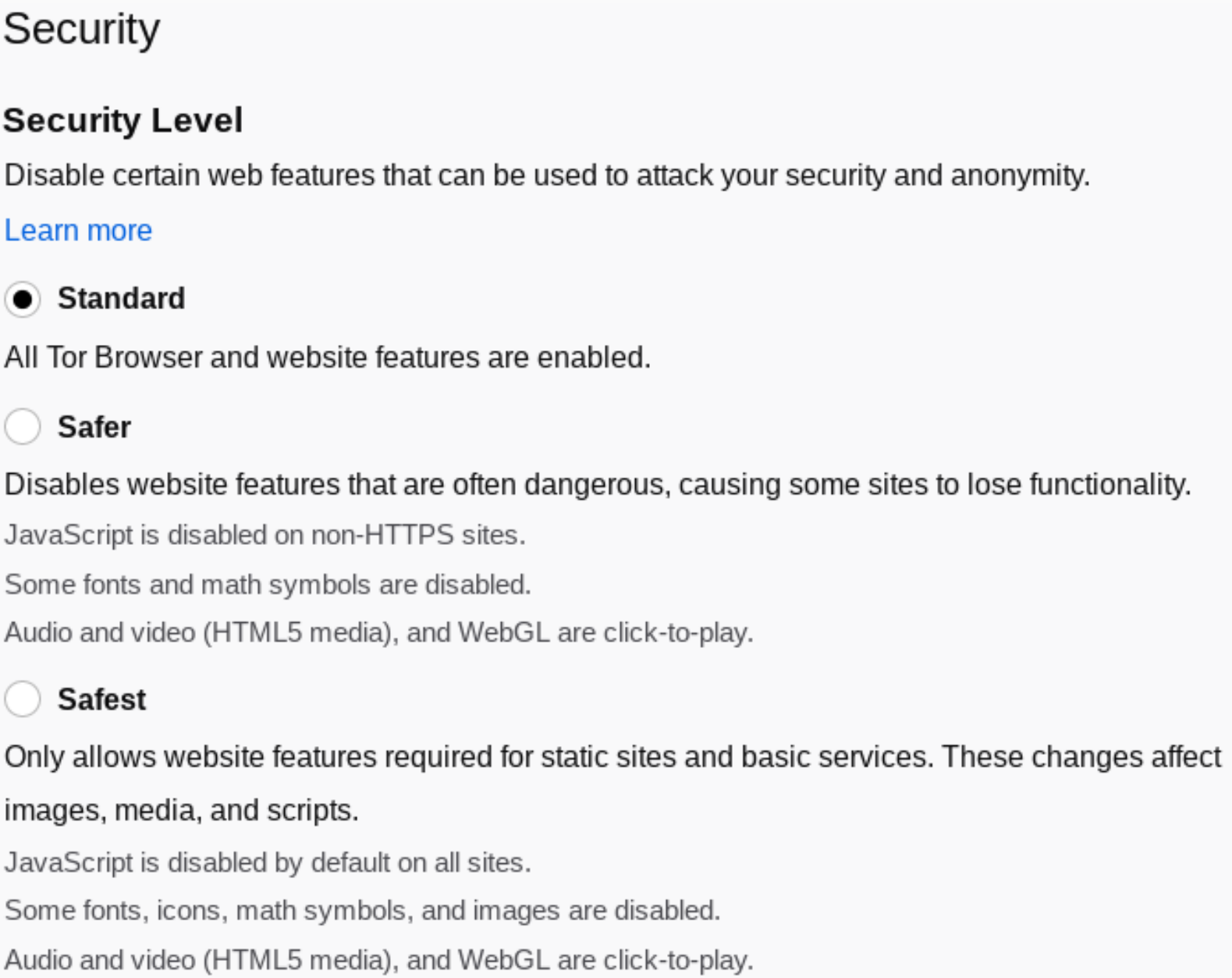
```
(function () {
  api.register(['audioFormats', 'audioContext', 'analys
  /*#__PURE__*/
  regeneratorRuntime.mark(function _callee() {
    return regeneratorRuntime.wrap(function _callee$(_c
      while (1) {
        switch (_context.prev = _context.next) {
          case 0:
            _context.t0 = getAudioFormats();
            _context.t1 = getAudioContext();
            _context.t2 = getAnalyserNode();

            if (!(navigator.userAgent.includes('Chrome
              _context.next = 7;
              break;
```

Browser Fingerprinting: Javascript

Browser Fingerprinting: TBB



Browser Fingerprinting: TBB



Browser Fingerprinting: Solutions

Browser Fingerprinting: Solutions

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

Demo

https://tails.boum.org/

References

- `https://github.com/Attacks-on-Tor/Attacks-on-Tor`
- Slides from George Danezis, University College London