What is Internet Filtering?

• Is a form of non-democratic oppression on people

• It allows those in power to subvert reality
FilterNet

- It’s a distortion of what is in reality the internet.
- Follows the subjectiveness of the authorities
- This does not help humanity
There is no just censorship.

- Internet filtering is happening in China, Iran, Syria, but also in Italy, UK, Netherlands.
- The only solution to what is considered by some wrong information is more information.
What we are doing?

• Help people access information Anonymously (Tor)
• Help people circumvent censorship (Tor, Tor Bridges)
• Measure Internet filtering in the world (OONI-Probe)
• Help people speak freely and anonymously (Tor Hidden Services, APAF)
Brief Timeline of Tor Censorship

• 2002 - The Source code for Tor is released
• 2006, April - Thailand - DNS Filtering of Tor
• 2006 - Websense/netfilter - Block Tor based on Tor GET requests
• 2007 - Iran, Saudi - Blocks Tor thanks to Websense
• 2009, Tunisia - Smartfilter to block all except 443, 80
• XXX - Tor bridges are introduced
**How Tor Works: 1**

Step 1: Alice’s Tor client obtains a list of Tor nodes from a directory server.

- Alice
- Dave
- Jane
- Bob

**How Tor Works: 2**

Step 2: Alice’s Tor client picks a random path to the destination server. Green links are encrypted, red links are in the clear.

- Alice
- Jane
- Dave
- Bob

**How Tor Works: 3**

Step 3: If at a later time, the user visits another site, Alice’s Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

- Alice
- Jane
- Dave
- Bob
getTor

• Tor software downloads are currently blocked from China, Iran, Lebanon, Qatar, etc.

• Tor delivers via email, write to gettor@torproject.org and we will send you a client to bootstrap a Tor client

• learn more: https://torproject.org/
Tor Bridges

- When the Tor network is blocked you can use bridges
- They are not published so it makes them harder to block
- learn more: https://www.torproject.org/docs/bridges
Existing filter detection tools

- Various captive portal software
  - Windows/iOS/Android/Google Chrome
- ONI has a tool called “rTurtle”
  - ...
- Herdicit “The verdict of the herd”
  - ...
- Some academic research
  - GATech and UC Berkeley have the best work
- Methodology, tools and data are (usually) closed
ooni-probe: Measuring filtering

- Open Observatory of Network Interference
- Provide a methodology and framework
- Make our data and code publicly available
What it detects

• It’s goals is to detect:
  • Network filtering (“Is my network traffic being tampered with?”)
  • Content restrictions (“What is being blocked?”)
  • Filtering technique (“How is it being blocked?”, “What software are they using?”)
Architecture

Work Unit
- Assets
- Test

Node

Report

OONI-net

Backend
- HTTP
- traceroute
- DNS
- echo
- Reports
Network filtering detection

- **Two way traceroute** If there is a difference between an inbound traceroute and an outbound traceroute for certain source and destination ports this may be an indication of traffic being routed to interception devices.

- **Header field manipulation** By varying the capitalization and adding certain headers to layer 7 protocols it is possible to detect on the receiving end if the traffic has been tampered with.
Filtered content tests

- **HTTP Host** This involves changing the Host header field of an HTTP request to that of the site one wishes to check for censorship.

- **DNS lookup** This involves doing a DNS lookup for the in question hostname. If the lookup result does not match the expected result the site is marked as being censored.

- **Keyword filtering** This involves sending an receiving data that contains certain keywords and matching for censorship. It is possible to use bisection method to understand what subset of keywords are triggering the filter.

- **HTTP scan** This involves doing a full connection to the in question site. If the content does not match the expected result then a censored flag is raised.

- **Traceroute** This involves doing TCP, UDP, ICMP traceroute for certain destination addresses if there are discrepancies in the paths with locations in the vicinities then a censorship flag is raised.

- **RST packet detection** This involves attempting to connect to a certain destination and checking if the client gets back a RST packet.
T-Mobile USA Web Guard

Wed 21 Mar 2012

T-Mobile USA offers a "feature" to restrict access to certain kinds of content. This is called Web Guard. Supposedly Web Guard is supposed to inhibit access to content that falls under the following categories: Alcohol, Mature Content, Violence, Drugs, Pornography, Weapons, Gambling, Suicide, Guns, Hate, Tobacco, Ammunition.

By developing an OONI-probe test we were able to extract part of the list of censored content and discovered that sites that do not fall under these categories were also censored. This feature is enabled by default on all prepaid accounts and although it can be disabled by customers who wish to do so (if over 18 years of age), it is not clearly stated in the error page how to do so. This means that T-Mobile USA customers may be drawn into the Filternet without knowing how to get out.

How is the censorship performed?
The technique being used by T-Mobile USA to restrict access to certain content involves deploying a transparent HTTP proxy. This proxy intercepts every HTTP packet going through the network and checks it's Host header field to see if it on the censored list. If the site is to be blocked it injects a fake response warning the user of the block. What this means is that the block is only effective against unencrypted HTTP traffic, but does not work for encrypted HTTPs traffic.

Some sites should not be censored
While most of the censored sites are legitimately categorized, there are certain ones that do not fall under the categories of the block. Here is a list of sites that we found to be censored, but that we don't believe belong to any of the following categories Alcohol, Mature Content, Violence, Drugs, Pornography, Weapons, Gambling, Suicide, Guns, Hate, Tobacco, Ammunition.
Handara Palestine

- 23 April 2012, released report on politically motivated censorship
- 27 April 2012, Palestinian minister of Communications resigns
- 5 May 2012, Censorship removed
Tor Hidden Services

- Anonymity for the server
- eqt5g4fuenphqinx.onion
- End-to-end encryption
Why use Hidden Service?

- Avoid retaliation for what you publish
- Securely serve content
- Stealth Hidden Services
Tor2web

- Allows Tor Web HS to be accessible from the world
- Instead of xxxxxxx.onion you use xxxxx.tor2web.org
- Tradeoff between security and anonymity for usability
Tor2web 1.0 issues

- Exposed to abuse complaints
- Misuse of HS to spread of illicit content
- No disclaimer
- No reporting system
- High latency -> Little usability
- The leads to server takedown
Tor2web 1.0
bodycount

• In 2010 there where at one point 3 tor2web nodes

• In April 2011, there was only one server left

• In June 2011, the last of the 3 original tor2web nodes went offline
This is the example page for Tor's rendezvous points system.

Read Thomas Paine's Common Sense.

Or read The Federalist papers, which were also originally published anonymously.
Future of tor2web

- Distribute responsibility
- Rewrite the code
- Get more Tor2web node!
tor2web mode

- An experimental implementation will be in tor 0.2.3.x
- Compile time flag --enable-tor2web-mode
Multidomain

- To run a tor2web node currently we need to entrust you with the wildcard SSL cert
- You should be able to run tor2web on xxxx.your_domain.org
- There can be a list of all supported tor2web domains
We need more nodes!

- Do you have a dedicated IP space?
- Do you want to help support tor2web network?
- Currently there is only 1 tor2web node :(
Legal help

• Write good Terms of Service

• Any lawyer interested in helping out?