How governments have tried to block Tor

Roger Dingledine

The Tor Project

https://torproject.org/
What is Tor?

Online anonymity 1) open source software, 2) network, 3) protocol
Community of researchers, developers, users, and relay operators
Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, NSF, US State Dept, SIDA, ...
The Tor Project, Inc.

U.S. 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
Estimated ~400,000 daily Tor users
Threat model: what can the attacker do?

Alice

Anonymity network

Bob

watch Alice!

Control part of the network!

watch (or be!) Bob!
Anonymity isn't encryption: Encryption just protects contents.
Anonymity isn't just wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

“Promise you won't remember!”

“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”
Anonymity serves different interests for different user groups.

“It's privacy!”
Anonymity serves different interests for different user groups.

- Private citizens: “It's privacy!”
- Businesses: “It's network security!”

Anonymity
Anonymity serves different interests for different user groups.

“*It's traffic-analysis resistance!*”

Governments

Anonymity

Private citizens

“*It's privacy!*”

Businesses

“*It's network security!*”
Anonymity serves different interests for different user groups.

- **Governments**: “It's traffic-analysis resistance!”
- **Human rights activists**: “It's reachability!”
- **Businesses**: “It's network security!”
- **Private citizens**: “It's privacy!”
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a single relay (or eavesdropper!) is a single point of failure.

E(Bob3, “X”)  E(Bob1, “Y”)  E(Bob2, “Z”)  “Y”  “Z”  “X”
… or a single point of bypass.

Timing analysis bridges all connections through relay ⇒ An attractive fat target
So, add multiple relays so that no single one can betray Alice.
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Number of relays

The Tor Project - https://metrics.torproject.org/
Tor's code released (2002)

- Tor's code released in 2002
- Tor's design paper published in 2004
- The clock starts ticking...
Thailand (April 2006)

- DNS filtering of our website
- Only by ISPs that participated in the Cyber Clean program of the Ministry of Information and Communication Technology
- Redirected to block page
Smartfilter/Websense (2006)

- Tor used TLS for its encrypted connection, and HTTP for fetching directory info.
- Smartfilter just cut all HTTP GET requests for “/tor/...”
  - That is not much of an arms race...
- Websense, Cisco, etc advertised this way of blocking Tor, even when it was obsolete.
Iran/Saudi Arabia/etc (2007)

- Picked up these Smartfilter/Websense rules by pulling an update
- The fix was to tunnel directory fetches inside the encrypted connection
  - When Iran kicked out Smartfilter in early 2009, Tor's old (non-TLS) directory fetches worked again!
Iran throttles SSL (June 2009)

- We made Tor's TLS handshake look like Firefox+Apache.
- So when Iran freaked out and throttled SSL bandwidth by DPI in summer 2009, they got Tor for free
Tunisia (summer 2009)

- As of the summer of 2009, Tunisia used Smartfilter to filter every port but 80 and 443.
- And if they didn't like you, they would block 443 just for you.
- You could use a Tor bridge on port 80, but couldn't bootstrap into the main network.
- So we set up a Tor directory authority doing TLS on port 80.
China (September 2009)

- China grabbed the list of public relays and blocked them
- They also enumerated one of the three bridge buckets (the ones available via https://bridges.torproject.org/)
- But they missed the other bridge buckets.
Relay versus Discovery

There are two pieces to all these “proxying” schemes:

a relay component: building circuits, sending traffic over them, getting the crypto right

a discovery component: learning what relays are available
The basic Tor design uses a simple centralized directory protocol.

Servers publish self-signed descriptors.

Authorities publish a consensus list of all descriptors.

Alice downloads consensus and descriptors from anywhere.
How do you find a bridge?

1) https://bridges.torproject.org/ will tell you a few based on time and your IP address

2) Mail bridges@torproject.org from a gmail address and we'll send you a few

3) I mail some to a friend in Shanghai who distributes them via his social network

4) You can set up your own private bridge and tell your target users directly
Attackers can block users from connecting to the Tor network

1) By blocking the directory authorities
2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services
3) By filtering based on Tor's network fingerprint
4) By preventing users from finding the Tor software (usually by blocking website)
Sorry, the requested page is unavailable.

If you believe the requested page should not be blocked please click here.

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa

Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.
China (March 2010)

- China enumerated the second of our three bridge buckets (the ones available at bridges@torproject.org via Gmail)
- We were down to the social network distribution strategy, and the private bridges
Bridge users from China

The Tor Project - https://metrics.torproject.org/
Iran (January 2011)

- Iran blocked Tor by DPI for SSL and filtering our Diffie-Hellman parameter.
- The prime $p$ recommended by the DNSSEC RFC is part of a banned class of numbers.
- Socks proxy worked fine the whole time (the DPI didn't pick it up).
- DH $p$ is a server-side parameter, so the relays and bridges had to upgrade, but not the clients.
Directly connecting users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
Egypt (January 2011)

- Egypt selected and targeted sites for blocking
  - Twitter was not entirely blocked but the attempt was good enough
- When Egypt unplugged its Internet, no more Tor either.
Directly connecting users from Egypt

The Tor Project - https://metrics.torproject.org/
Libya (March-July 2011)

• Libya might as well have unplugged its Internet.
• But they did it through throttling, so nobody cared.
Syria (June 2011)

- One ISP briefly DPIed for Tor's TLS renegotiation and killed the connections.
- A week later, that ISP went offline. When it came back, no more Tor filters.
- Who was testing what?
Directly connecting users from the Syrian Arab Republic

The Tor Project - https://metrics.torproject.org/
Iran (September 2011)

- This time, DPI for SSL and look at our TLS certificate lifetime.
- (Tor rotated its TLS certificates every 2 hours, because key rotation is good, right?)
- Now our certificates last for a year
- These are all low-hanging fruit. How do we want the arms race to go?
Directly connecting users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
Top-3 countries by directly connecting daily Tor users

The Tor Project - https://metrics.torproject.org/
China (October 2011)

- China DPIs for SSL + Tor's ciphersuites, does active follow-up probing that talks the Tor protocol!
- Two avenues to solving it:
  - Change ciphersuite to blend in better
  - Scanning-resistance
Iran (February 2012)

- DPI for all SSL flows and cut them
- No more gmail, facebook, etc etc
- Pluggable transports
  - Obfsproxy
  - SkypeMorph
  - StegoTorus
- Need “obfuscation” metrics?
Directly connecting users from Iran

The Tor Project - https://metrics.torproject.org/
What we're up against

Govt firewalls used to be stateless. Now they're buying fancier hardware.
Burma vs Iran vs China
New filtering techniques spread by commercial (American) companies :(
Tor's safety comes from diversity

- **#1**: Diversity of relays. The more relays we have and the more diverse they, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)

- **#2**: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.
Only a piece of the puzzle

Assume the users aren't attacked by their hardware and software
No spyware installed, no cameras watching their screens, etc
Users can fetch a genuine copy of Tor?
BridgeDB needs a feedback cycle

- Measure how much use each bridge sees
- Measure bridge blocking
- Then adapt bridge distribution to favor efficient distribution channels
- (Need to invent new distribution channels)
I CAN HAZ FREEDOM?

Tor
TorProject.org
Next steps

Technical solutions won't solve the whole censorship problem. After all, firewalls are *socially* very successful in these countries. But a strong technical solution is still a critical puzzle piece.

You should run a relay! Non-exit relays are easy and safe to set up.