How governments have tried to block Tor

Roger Dingledine
Jacob Appelbaum
The Tor Project
https://torproject.org/
Estimated ~400,000 daily Tor users
Threat model: what can the attacker do?

- Alice
  - Watch Alice!
- Anonymity network
  - Control part of the network!
- Bob
  - Watch (or be!) Bob!
Number of relays

The Tor Project - https://metrics.torproject.org/
Context is everything

This conference is perfectly themed for our subject matter.
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.
  - We also now have a dynamic prime option
- 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 (Jacob's authority urras).
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.

S1

S2

S3

Servers publish self-signed descriptors.

Trusted directory

Trusted directory

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.

Access to this website is prohibited

This site has been blocked.

The web page you are trying to access has been blocked as the content contains prohibited materials.

أوُجِبَتُتْ قُدُمُكَ لِلْمَعْطِفَةِ

تَحَكُّمُتْ فِي الْفَيْضَةِ

يُقَدِّسُ النَّفْعُ عَلَيْهِ

لِتَوَكِّفَ الْقُرْةِ

لِتَقْنَى النَّفْعُ عَلَيْهِ

لِتُقَدِّسُ النَّفْعُ عَلَيْهِ

لِتَوَكِّفَ الْقُرْةِ

لِتَقْنَى النَّفْعُ عَلَيْهِ

لِتُقَدِّسُ النَّفْعُ عَلَيْهِ
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
Greece (~5th century BC)

• Jumping back in time...
  – Hippasus is drowned for showing a new class of numbers...
    • “Proof of the irrationality of $\sqrt{2}$”
Iran (January 2011)

- Iran blocked Tor by DPI for SSL and filtering our Diffie-Hellman parameter.
  - Our prime $p$ is part of a banned class of numbers; not irrational, liberating?
- 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 (TEData)
• 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.
Directly connecting users from Libya

The Tor Project - https://metrics.torproject.org/
Syria (June 2011)

- One ISP briefly DPIed for Tor's TLS renegotiation and killed the connections.
  - Blue Coat, more like *Red Coats*!
- 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/
A tale of two circumvention systems

- Ultrasurf
  - Distinguishable behavior
  - Lots of unnecessary data in logs
  - Evidence of unproxied traffic
- Tor
  - Looks like SSL
  - No extra details in logs
Bluecoat logs from Syria (worse)

- 2011-08-05 23:45:19 539 31.9.244.83 - - - OBSERVED "unavailable" - 200 TCP_NC_MISS GET text/html; %20charset=UTF-8 http 74.125.39.106 80 /gwt/n? u=http://114.42.119.186/MzYwOWEwMjZn/k6IPd6kevXg2/1KQEH7fij/XAojkR9c/14g2SRugC7Hx/vba1vA - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 82.137.200.44 2409 230 -
Bluecoat logs from Syria (better)

- 2011-08-05 23:52:31 166849 82.137.249.41 - - - OBSERVED "unavailable" - 200 TCP_TUNNELED CONNECT - tcp 208.83.223.34 80 / - - - 82.137.200.44 4086 2657 -
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/
October 2011 advances?

- Iran DPIs for SSL, recognizes Tor, and throttles rather than blocks?
- China DPIs for SSL, does active follow-up probing to see what sort of SSL it is?
- https://trac.torproject.org/projects/tor/ticket/4185
December 2011

Reports of redirection of traffic in Iran to peyvandha.ir
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 :(
How to separate “oppressing employees” vs “oppressing citizens” arms race?
  – What's the difference anyway?
What we're up against

Blue Coat
SmartFilter
Websense
Nokia
Cisco

And many many more (See Jacob's RECon2011 talk for more details)
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. 40000 users in Iran means almost all of them are normal citizens.
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)
Measuring bridge reachability

- Passive: bridges track incoming connections by country; clients self-report blockage (via some other bridge)
- Active: scan bridges from within the country; measure remotely via FTP reflectors
- Bridges test for duplex blocking
Other components

Traffic camouflaging

Super-encrypt so no recognizable bytes?
Shape like HTTP?

We're working on a modular transport API

Need “obfuscation” metrics?
We must reject so-called “lawful interception” and data retention

To understand the scope of the market and the reach of the market - we encourage you to look at the BuggedPlanet Wiki and to read about the WikiLeaks release of the Spyfiles:

http://spyfiles.org/
http://buggedplanet.info/
I CAN HAZ FREEDOM?

Tor
TorProject.org