The Future of Anonymity and Censorship Resistant Publishing

Steven J. Murdoch

http://www.cl.cam.ac.uk/users/sjm217
Many countries censor the Internet

- Out of the 40 countries studied by the OpenNet Initiative in 2006, 26 censored the Internet in some way.
- The types of material censored varied depending on country, for example:
  - Human Rights (blocked in China)
  - Religion (blocked in Saudi Arabia, UAE, Iran, Bahrain)
  - Pornography (blocked in Saudi Arabia, UAE, Iran, Bahrain, Singapore, Burma, ...)
- Other issues censored include: military and militant websites; sex education, alcohol/drugs, music; gay and lesbian websites; news, online communities.
Many countries censor the Internet

- Out of the 40 countries studied by the OpenNet Initiative in 2006, 26 censored the Internet in some way
- The types of material censored varied depending on country, for example:
  - Human Rights (blocked in China)
  - Religion (blocked in Saudi Arabia, UAE, Iran, Bahrain)
  - Pornography (blocked in Saudi Arabia, UAE, Iran, Bahrain, Singapore, Burma, ...)
- Other issues censored include: military and militant websites; sex education, alcohol/drugs, music; gay and lesbian websites; news, online communities
Many countries censor the Internet

- Out of the 40 countries studied by the OpenNet Initiative in 2006, 26 censored the Internet in some way.
- The types of material censored varied depending on country, for example:
  - Human Rights (blocked in China)
  - Religion (blocked in Saudi Arabia, UAE, Iran, Bahrain)
  - Pornography (blocked in Saudi Arabia, UAE, Iran, Bahrain, Singapore, Burma, ...)
- Other issues censored include: military and militant websites; sex education, alcohol/drugs, music; gay and lesbian websites; news, online communities.
Even if a site is accessible, it may be removed from search engine results.

Searching for “Tiananmen Square” on Google.com and Google.cn
Self-censorship can be very effective

- Circumvention technologies are far ahead of blocking, anyone sufficiently motivated will be able to bypass existing blocking techniques
- But blocking remains effective because of self-censorship and reluctance to use circumvention
- The fact that users are circumventing blocking can be detected and social/legal pressure can be applied. Even the risk of prosecution can be an effective deterrent
Anonymity systems hide their users communication patterns

- Anonymity systems protect their users by hiding:
  - The content (what is being said)
  - The traffic data (who is communicating with whom)
- In the case of a website, it should be possible to use an anonymity system to:
  - Hide what information is being sent to and from that website
  - Hide who is accessing the website from the operator of the website
  - Hide who is operating the website
- Examples of anonymity systems include:
  - Mixmaster and Mixminion (for email)
  - Freenet (for file sharing)
  - Tor (for web browsing, instant messaging, ...)
Anonymity systems are closely linked to censorship resistance

- If nobody can tell what you are accessing, censors cannot block selected material
- If nobody can tell who is accessing or publishing banned material, the users are protected from selective punishment

However, anonymity systems are only one component of a censorship resistance system

- Users must find the necessary software (many countries block the normal software distribution site)
- The anonymity system must avoid being blocked itself
- Users must be trained to use the software properly, and not be compromised by other methods (e.g. computer hacking, physical break-ins)
Tor hides communication patterns by relaying data through volunteer servers

Diagram: Robert Watson
Tor hides communication patterns by relaying data through volunteer servers
Tor hides communication patterns by relaying data through volunteer servers.
Tor hidden services allow censorship resistant hosting of services.
Tor implements censorship resistance

- A list of all Tor server is publicly visible, in order for users to build paths through the network
- This also makes it fairly easy for a country to block all Tor servers
- “Bridges” are special Tor nodes which are only known by a small number of users, which can be used to access the network

Here are your bridge relays:

bridge 222.129.55.204:443 88a09a6997a2b6e1f80e4e25b1d26d4b0af8ccfb
bridge 92.113.0.230:443 bcac0b1daf0895a33e7f607f4ea4e22c86ec5f9
bridge 71.207.219.190:443 51dacec1f3ccf35bd43b34988550a2af5c24163a

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.
Tor implements censorship resistance

- A list of all Tor server is publicly visible, in order for users to build paths through the network
- This also makes it fairly easy for a country to block all Tor servers
- “Bridges” are special Tor nodes which are only known by a small number of users, which can be used to access the network
Psiphon is censorship resistance system with different design tradeoffs to Tor

- There is no centralized control, so it is hard to block but also hard for user to find a server
- Users do not have to download software, but this limits the strength of protection
- If the user cannot modify browser settings or install software, Psiphon is still usable
- Users within a censored country can ask someone they trust outside of the country to install the Psiphon server
Freenet is an anonymous content distribution network

- While Tor and Psiphon allow access to the Internet, Freenet creates a private network
- Users can create websites, share files and send/receive emails between other members of the network
- Content is hosted by sharing it amongst users of the network
- Users cannot select what content they host, and it is stored in an encrypted form
Anonymity research is an active field

- Anonymity systems are unusual in that deployed systems are also the state-of-the-art in research, for example Mixminion and Tor
- Researchers are developing attacks, and corresponding defences, against weaknesses in the anonymity systems
- One of the most important classes of attacks is traffic analysis
- Here timings and volume of information are used to establish who is communicating with whom
- High-latency systems like Mixminion, where emails are delayed for hours or days, give good resistance to this attack
- With Tor, where latencies of more than a few seconds would be intolerable for web browsing is more vulnerable
- Simple censorship resistance systems, like Psiphon offer no protection against this attack
Tor servers are operated by volunteers, so someone malicious can inject their own malicious nodes.
If both the entry and exit servers are malicious, the user is at risk.
If both the entry and exit servers are malicious, the user is at risk.
Even though Tor encrypts data, timing of data transmissions is almost unchanged.

Malicious entry and exit nodes correlate traffic to de-anonymize connections through Tor.

Diagram: Robert Watson
Censorship resistance also introduces research challenges

How to distribute addresses of servers:
- To prevent servers from being blocked, it must be infeasible to enumerate all servers
- Currently Psiphon relies on existing social networks
- Tor gives out a few addresses to each IP or email address

How to distribute software:
- The Tor website is widely blocked, so getting Tor is difficult
- Users can also receive Tor by email, IRC or a mirror site

How to resist blocking by traffic fingerprinting:
- The first version of the Tor generated traffic that was easy to identify
- The current version looks quite like HTTPS web browsing
- More work is needed to make it look closer
Anonymity and censorship resistance software needs to be easy to use safely

- The Tor Browser Bundle is a simple way of getting Tor
- The Tor website is translated into many languages
- Guides and training on how to use Tor safely have been produced
Anonymity and censorship resistance software needs to be easy to use safely

- The Tor Browser Bundle is a simple way of getting Tor
- The Tor website is translated into many languages
- Guides and training on how to use Tor safely have been produced
Anonymity and censorship resistance software needs to be easy to use safely

- The Tor Browser Bundle is a simple way of getting Tor
- The Tor website is translated into many languages
- Guides and training on how to use Tor safely have been produced
Future developments

- While the current anonymity and censorship resistance systems are used by many people, there is room for improvement.
- Research on traffic analysis is needed to better understand attacks and design defences.
- Ways to grow the Tor network, while still preserving anonymity are needed to allow more users.
- We should establish how users understand anonymity, what they need, and how to more effectively teach them to be safe.
- ... and many more challenges.

How to get involved

- Look at the website, join the mailing lists.
- Write documentation, look for bugs, implement new features.
- Apply for the Google Summer of Code next year (hopefully).

https://www.torproject.org/