Censorship resistant technologies

Steven J. Murdoch
www.cl.cam.ac.uk/users/sjm217

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

OpenNet Initiative
www.opennet.net

Horizon seminar: Risk, Threat & Detection, 5 December 2006, Cambridge, UK
Summary

- What is blocked, who by and why?
- How does blocking work?
- How can such blocking be circumvented?
- Why is this insufficient?
- What is the future of censorship resistance?
• Human Rights in China
• Aung San Suu Kyi, leader of National League for Democracy, an opposition party in Burma
Human Rights in China

Aung San Suu Kyi, leader of National League for Democracy, an opposition party in Burma
Religion

- Sites aimed at religious conversion are sometimes blocked. This particular site is not accessible in Saudi Arabia.
- Christian websites which target Islamic audience are particularly liable to be filtered in some Middle Eastern countries. This site is additionally inaccessible in the UAE, Iran and Bahrain.
• Sites aimed at religious conversion are sometimes blocked. This particular site is not accessible in Saudi Arabia.

• Christian websites which target Islamic audience are particularly liable to be filtered in some Middle Eastern countries. This site is additionally inaccessible in the UAE, Iran and Bahrain.
• Blocked by several countries and sub-nationally (libraries, homes)
• Middle East (e.g. Bahrain, Saudi Arabia, Iran, Oman), Singapore, Burma/Myanmar . . .
• Convenient cover for other types of blocking
  • In Vietnam, the state claim that only obscene material is restricted, but testing revealed that while no pornography was blocked, political, religions and media websites were
• Governments can derive legitimacy by being seen to block content prohibited by the dominant religion
Many more issues

- Military and militant websites
- Sex education, alcohol/drugs, music
- Gay and lesbian websites
- News, online communities and chat
- Censorship circumvention
- Child pornography
- Nazi material
- ...
Explicit blocking

- Another way in which blocking regimes vary is how transparent the process is.
- In this example, from Saudi Arabia the fact that the site is blocked is clear, and the user may request unblocking.

Access to the requested URL is not allowed!
Disguised as errors

- In contrast, when a site or keyword is blocked in China, it will appear to be a network error.
- The situation is similar in Tunisia, where an the blocking system impersonates an Internet Explorer error message.
“In China, we don’t have software blocking Internet sites. Sometimes we have trouble accessing them. But that’s a different problem. … We do not have restriction at all.”

Chinese official at 2006 Internet Governance Forum, Athens
Blocking and proxy servers
Blocking and proxy servers
Blocking and proxy servers

Diagram:
- Web browser
- Firewall
- Internet
- Proxy server
- Blocked website
Types of proxy servers

- Some types require altering the configuration of the computer so may not be usable in Internet cafés.
- Unencrypted proxies will bypass most types of blocking, but the content of pages is available so keyword blocking will succeed.
- Encrypted proxies, such as Psiphon, do hide the content, but the operator of the proxy will still know who is browsing which website.
- Privacy software, such as Tor, will hide patterns of communication.
Types of proxy servers

- Some types require altering the configuration of the computer so may not be usable in Internet cafés.
- Unencrypted proxies will bypass most types of blocking, but the content of pages is available so keyword blocking will succeed.
- Encrypted proxies, such as Psiphon, do hide the content, but the operator of the proxy will still know who is browsing which website.
- Privacy software, such as Tor, will hide patterns of communication.
Privacy

- Undesirable content can be reliably blocked simply by cutting off the Internet, at cost of blocking desirable content too.
- Blocking can be resisted by hiding within content too valuable to block (e.g., e-commerce, online banking).
- Cannot hide by yourself, need a crowd with a variety of members.
- Privacy needed for many different reasons, and need each other for any of them to have privacy. E.g.
  - Censorship resistance
  - Police communicating with contacts
  - Intelligence organisations investigating terrorist websites
  - Human rights workers in the field
  - Internet Watch Foundation building list of child pornography
  - Companies monitoring competitors and potential take-over targets
- Tor started by US Navy, taken over by a civil rights organisation (EFF) and used by law enforcement, financial research, human rights workers, censored Internet users worldwide.
Why does filtering still work?

- 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
Future research

- Better understanding of censorship capabilities
- More reliable and comprehensive mechanisms for detecting censorship
- Surveillance resistant communications: improving usability and security