



Tools for Censorship Resistance

Rachel Greenstadt
greenie@eecs.harvard.edu

Defcon XII
July 29, 2004

<http://www.eecs.harvard.edu/greenie/defcon-slides.pdf>

Overview

- **Approaches to Censorship**
- Circumvention methods
- Case study: China
- Censorship in a “free” society
 - ▶ the LOCKSS project
- Unobservability

A Taxonomy of Censorship

- Generalized Blocking
 - ▶ Blocking publishers/servers
 - ▶ Blocking receivers/clients
 - ▶ Modifying content for censorship
 - ▶ "Arms race" solutions okay
- Surveillance/Chilling Effects
 - ▶ Relies on accountability/punishment

Effective censors use multiple techniques

Blocking Publishers



Figure 1: Bonsai kitten picture from bonsaikitten.com

- Hardest form of censorship to do (spam)
- Offensive material forbidden by govt/ISP/DOS attackers

Circumventing Publisher Blocking

- Find someone who will make material available
 - ▶ More permissive ISP
 - ▶ Writable web pages (blogs, etc)
 - ▶ Outside jurisdictions
- Anonymity services
 - ▶ Can help if publisher blocking is combined with surveillance
 - ▶ Hidden servers may prove useful for avoiding DOS attacks
 - ▶ Current systems probably too fragile

Blocking Receivers

If the blocking authority has control over some, but not all, internet users

- Government firewalls at routers
- Corporate firewalls
- Nannyware in schools/libraries

Blocking Approaches 1

Web Site Blocked

The website you were trying to access was deemed inappropriate by the Authorities. If you feel that this particular web site should not have been blocked per our policy, you may ask that the web site be removed from the blocked list by going to the following [website](#).

If you have any questions, contact us at internetpolice@authority.net.

Blocking Approaches 2

ERROR 404 - File Not Found



No there is no page here. There is no page within a hundred kilobytes of here.

I am not worried. And neither should you be.

In fact, as we speak, viruses are committing suicide outside the firewall of this server, and we encourage them to continue doing so.

There is only truth [HERE](#). All the rest is lies! Lies! Lies!

Iraq - 03/2003

Blocking Techniques

- Block open or closed?
- Drop packets at gateway based on IP address
- DNS redirection
- Filter based on keywords
- Filter based on images ("Finding Naked People")
- Block loophole servers
 - ▶ Proxies/anonymizers/translators/google cache/wayback machine/etc

Overview

- Approaches to Censorship
- **Circumvention methods**
- Case study: China
- Censorship in a “free” society
 - ▶ the LOCKSS project
- Unobservability

Circumvention Methods

- Proxies
- Tunnels
- Mirrors
- Email (spam)
- P2P systems to make proxies available
 - ▶ Safeweb/Triangle-Boy, Six/Four, Peek-a-booty, Infranet

Publicizing the circumvention system

You don't: used by small set of people, communicate out of band

Use something to communicate that they won't or can't block

- This may be harder than you think

Closed group: no one sees the whole pattern

- Intranet: keyspaces-hopping (client puzzles)
- TU Dresden: captchas
- Won't work against a resource rich adversary

Stego in Circumvention Systems

Can make proxy servers more difficult to detect and block, clients have plausible deniability

- Infranet (MIT NMS)—embed requests for content in the sequence of `http` requests, embed content itself steganographically in images
- Camera Shy (Hacktivismo)—uses `lsb` steganography. Automatically scans and parses web pages for applications

Tools

- Peacefire Circumventor: <http://www.peacefire.org>
- Psiphon: <http://www.citizenlab.org/>
- DIT: <http://www.dit-inc.us/>
- Anonymizer: <http://www.anonymizer.com/>
- TOR: <http://freehaven.net/tor/>
- Hacktivismo: <http://www.hacktivismo.com/>
- Freenet-china: <http://www.freenet-china.org/>

Overview

- Approaches to Censorship
- Circumvention methods
- **Case study: China**
- Censorship in a “free” society
 - ▶ the LOCKSS project
- Unobservability

Internet Censorship in China

- Use publisher/receiver blocking, surveillance
- Makes evident how much of “cyberspace” is tied to national borders and how much isn’t
- Opaque system, closed blocking

Goals

Block dissident websites and pornography

- Belief that access to the Internet would foment change/unrest
- Also—Internet used as coordination tool for dissidents
- 3 main dissident groups (Rand)
 - ▶ Falun Gong
 - ▶ Chinese Democratic Party
 - ▶ Tibetan/Taiwanese sites
- Also block news, health, education, gov't, religion

PRC Resources

- Control of routers inside China
- Internet access in country through cooperative ISPs
- Sophisticated network and Internet cafe surveillance
- approx 30,000+ employees to find sites to filter (Big Mamas/volunteers)
- Ability to arrest/detain/interrogate suspicious individuals

Evolution of Chinese Censorship

Witnessing the “arms race”

- | | |
|------|---|
| 1995 | Internet commercially available in China |
| 1996 | “Great Firewall of China” |
| 1997 | Regulations place liability for Internet use on ISPs |
| 1999 | Foreign dissident sites DOS’ed |
| 2000 | Golden Shield begins, Security China 2000 |
| 2001 | Safeweb/Triangle Boy blocked |
| 2001 | Capital crime to “provide state secrets” over Internet |
| 2002 | Pledge of Self-Discipline for Chinese Internet Industry |
| 2002 | DNS hijacking |

Evolution of Chinese Censorship

- | | |
|------|---|
| 2002 | Attempt to block google -> keyword blocking |
| 2002 | More fine grained blocking (CNN, blogspot) |
| 2002 | Internet cafe fi re, PRC closes cafes |
| 2002 | Cafes required to install surveillance software |
| 2002 | Downtime punishment |
| 2004 | est. 87 million Internet users in China |
| 2004 | PRC monitoring SMS text messages |

Sad Story of Safeweb

- Set up a proxy service, got blocked
- Set a P2P network of proxies, they got blocked
- Almost immediately
- With their resources, China can discover the peers and block them, even with rate limiting measures
- You try getting a P2P network up and running this way
- Involuntary servers? (In a windows app?)
 - ▶ On a safe port—blocked
 - ▶ A gazillion IIS servers, there's a good idea...

But they wouldn't block X...

- Only a few sites they unblocked (google, blogspot)
- Even these they do selective blocking
- And random P2P servers aren't likely to be useful to them for anything
- Don't expect companies to help you
 - ▶ We're selling them surveillance tech
 - ▶ They've signed self-discipline pledges too

VIP Reference

- Dissident email newsletter
(<http://come.to/dck>)
- Most successful widespread circumvention
- Spam's a hard problem
- Sent to prominent party members, random Chinese, and dissidents
- Not without repercussions: Lin Hai sentenced to 2 years in prison for providing 30,000 email addresses to “overseas hostile publications”

Implications Outside China

- Traffic routed through China subject to filtering
- Root nameserver in China could cause people outside China to be subject to DNS hijacking
- Common carrier status?

References on China

- “Empirical Analysis of Internet Filtering in China,” Zittrain/Edelman, Harvard Berkman Center
 - ▶ Zittrain/Edelman, Harvard Berkman Center
 - ▶ <http://cyber.law.harvard.edu/filtering/china/>
- “You’ve Got Dissent! Chinese Dissident Use of the Internet and Beijing’s Counter-Strategies”
 - ▶ Chase/Mulvenon, RAND
 - ▶ <http://www.rand.org/publications/MR/MR1543/>

Overview

- Approaches to Censorship
- Circumvention methods
- Case study: China
- **Censorship in a “free” society**
 - ▶ the LOCKSS project
- Unobservability

Document distortion or removal

- Form of blocking, previously available items are changed or disappear
- Concern in U.S. (talk at PORTIA)
- Can be mitigated with digital signatures
- BUT—Often self-censorship

Example: Time Magazine



- This article was removed from Time's online website
- Also excised from the Table of Contents
- From memoryhole.org

LOCKSS: Lots of Copies Keep Stuff Safe

- Libraries help prevent document distortion by preserving documents in many locations
- LOCKSS is a P2P system to help libraries
 - ▶ Archive documents and avoid bit rot
 - ▶ Maintain consensus about which document is correct
- Some online sources doing similar things (wayback machine, memoryhole, cryptome, google cache)

Overview

- Approaches to Censorship
- Circumvention methods
- Case study: China
- Censorship in a “free” society
 - ▶ the LOCKSS project
- **Unobservability**

Unobservability as Censorship Resistance

- Unobservability hides both the content and the fact that covert communication is taking place
- Examples: steganography, covert channels
- Can help circumvent surveillance
- And blocking (can't block what you don't know is there)
- Dissident two-way communication

Limitations of Encryption

- It may be forbidden, or bring unwelcome suspicion
- Censoring authority may have the ability to gain keys (Britain)
 - ▶ Many systems built to avoid this problem
- Requires some degree of coordination(keys)/technical sophistication

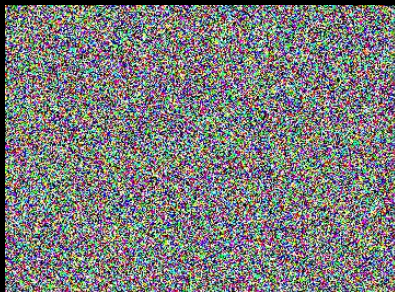
Properties for Unobservable Systems

- Undetectability
 - ▶ Plausible (legitimate cover)
 - ▶ Encode the message to match channel statistically
- Robustness
 - ▶ Message survive natural/malicious lossiness
 - ▶ Indispensable

Limitations of Unobservability

- Hard to have security guarantees about detectability
- Many 'unobservable' approaches are detectable—security through obscurity
- Especially true if you are worried about the channel being blocked

Pitfalls of Randomness



- Images from Westfeld's attacks on steganographic systems
- Embedding cryptographic output in nonrandom sources is obvious
- In general, bits are not random
- I made this mistake with TCP timestamps

Image Steganography

- LSB steganography is detectable. Easily.
- Increasingly good blind jpeg steg detection (Fridrich)
- Certainly an arms race
- Robustness?
- Image choice steganography
 - ▶ Very low bandwidth
 - ▶ But robust, hard to detect
 - ▶ Fotoblogs...

Conclusions

- Circumvention is easy to do on small scale, hard to do on large scale
- Hardest problem is distributing circumvention systems, without having them blocked
- Arms race double edged
 - ▶ Can cause working circumvention methods to get blocked
 - ▶ Make circumventor pay higher price for control
 - ▶ With surveillance, need to make sure users aware of risks