Evading Internet censorship

March 18, 2004

Topics

- Social issues
  - Internet censorship in US, China, Saudi Arabia. Restriction of what you can visit, or just monitoring of where you visit.
- Other work
  - Crowds, Anonymizer, Triangle Boy, Freenet, Mixminion...
- Infranet

Filtering in Saudi Arabia

- Saudi government controls link between the country and the rest of the Internet
  - According to Nov 2001 NY Times article, Saudi Arabia seeking bids from US companies to provide filtering technology.
  - All web traffic is forwarded through content filtering proxy servers.

- Material from: Jonathan Zittrain and Benjamin Edelman, Berkman Center for Internet & Society at Harvard Law School (http://cyber.law.harvard.edu/filtering/saudiarabia)

Saudi Arabia

- Banned pages: sexually explicit sites, plus “pages related to drugs, bombs, alcohol, gambling and pages insulting the Islamic religion or the Saudi laws and regulations."
- No public list available of the pages that are blocked (this is a common theme for web filters).
- Obviously, Anonymizer type services are blocked as well as translation services like Babelfish.

Role of US companies

- Cisco involved with firewall deployments in China - rumored to be working with China to help monitor user activity.
- Customized version of Yahoo! in China.

United States

- Content filters must be installed in both libraries and schools in order for them to receive certain federal subsidies (CIPA: The Children's Internet Protection Act).
    - Constitutionality challenged by ALA and others - law upheld by Supreme Court last June.
- Other similar laws: Child Pornography Prevention Act and Child Online Protection Act

Content filtering problems

- Biggest problem - who decides what pages to block?
  - All the major filtering packages have their own encrypted blacklists, usually divided into categories.
    - List is considered a trade secret - accessing it is a DMCA violation.
    - Content could be shaped by political or religious views.
- Can "whitelist" in mistakenly blocked sites.

Anonymity technologies

- Anonymizer.com
  - Easy to use. However, this and any other well-known services are easy for filtering proxies to block.
- An improvement: Triangle Boy (safeweb.com)
  - Gives access to SafeWeb's anonymizer service through third parties to get around filters.
  - Backed by CIA venture capital, and by Voice of America.

Other work

- Crowds - large group issues requests - hard to associate a request with the originating user
- Freenet - decentralized, anonymous content storage and retrieval
  - Each user donates bandwidth and disk space, but has no control over what specific content is located on their machine
- Mixminion - Type III anonymous remailer

There must be a better way!

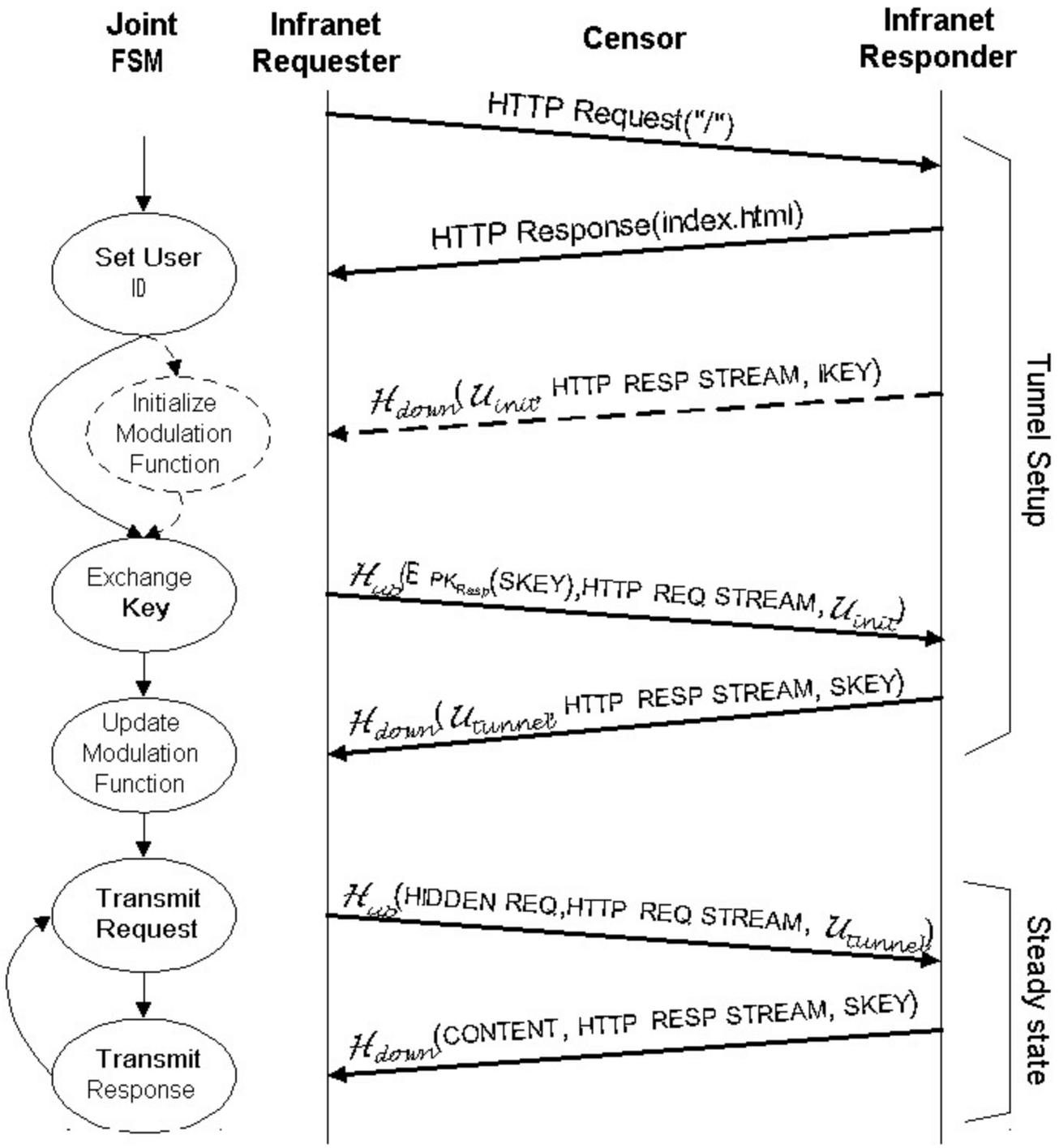
- Deniability
- Covertness
- Communication Robustness
- Performance

Announcing *Infranet*

- Requester
  - Local Proxy
- Responder
  - HTTP Server

Setup

- Set User ID
- Key Exchange
- Agree on Modulation Function

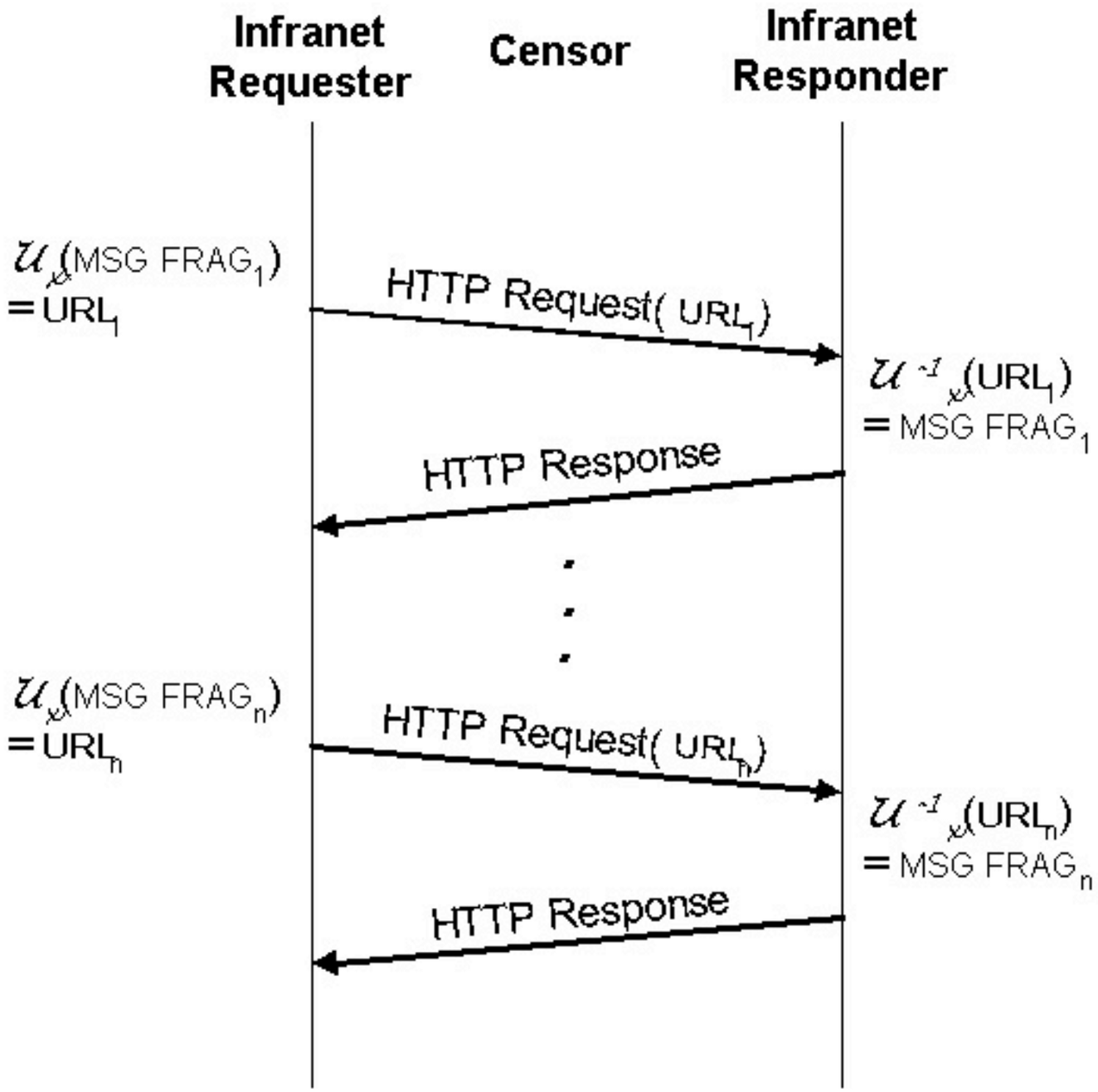

Joint FSM
Infranet Requester
Censor
Infranet Responder
HTTP Request("/")
HTTP Response(index.html)
Set User ID
Initialize Modulation Function
$\mathcal{H}_{down}(\mathcal{U}_{init}$ HTTP RESP STREAM, IKEY)
Exchange Key
$\mathcal{H}_{up}$(E PK_{Resp}(SKEY),HTTP REQ STREAM, $\mathcal{U}_{init}$)
Update Modulation Function
$\mathcal{H}_{down}(\mathcal{U}_{tunnel}$ HTTP RESP STREAM, SKEY)
Tunnel Setup
Transmit Request
$\mathcal{H}_{up}$(HIDDEN REQ,HTTP REQ STREAM, $\mathcal{U}_{tunnel}$)
Transmit Response
$\mathcal{H}_{down}$(CONTENT, HTTP RESP STREAM, SKEY)
Steady state

Upstream

- Implicit Mapping
  - Following Links:
    - e.g. Odd links -> ‘0’
    - Even links -> ‘1’
- Dictionaries
  - Responder sends a codebook
    - Static
    - Dynamic

Upstream

- Range-mapping
- Dictionary-based
- Multiple mappings enable better entropy
- Transactions look similar to standard HTTP traffic


Infranet Requester
Censor
Infranet Responder
$\mathcal{U}_{\mathcal{K}}$(MSG FRAG$_1$) = URL$_1$
HTTP Request(URL$_1$)
$\mathcal{U}^{-1}_{\mathcal{K}}$(URL$_1$) = MSG FRAG$_1$
HTTP Response
$\mathcal{U}_{\mathcal{K}}$(MSG FRAG$_n$) = URL$_n$
HTTP Request(URL$_n$)
$\mathcal{U}^{-1}_{\mathcal{K}}$(URL$_n$) = MSG FRAG$_n$
HTTP Response

Downstream

- JPEG Images
  - Redundant bits
    - Secret key
- Arousing Suspicion
  - Get HTML
  - Webcam

Security Analysis

- Insider Attacks
- Passive Attacks
  - Suspicious Content
    - Pattern Analysis
- Disruptive Attacks
  - Filtering
  - Transaction Tampering
  - Session Tampering