Privacy:- anonymity, ~~and~~ confidentiality, anti-censorship.

- Anonymous routing.
- Confidentiality + Anonymity
- Censorship resistance (and privacy)

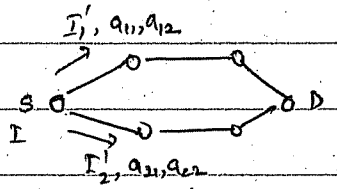
Goal: ability to send confidential anonymous messages.
- only the source and destination know the message content.
- network intermediaries do not know who is communicating.

- Anonymous routing on top of overlay — TOR
  1. uses private, public keys to establish symmetric keys
  2. uses symmetric keys to construct onion routes.

Problem: - trusted data based of nodes.
- key management. } big challenge

- Can you do it without keys? → can use random overlays for anonymous comm.
  get both confidentiality and anonymity.

Confidentiality → information slicing



$I \longrightarrow I_1, I_2 \rightarrow \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \end{bmatrix} \rightarrow \begin{bmatrix} I_1' \\ I_2' \end{bmatrix}$

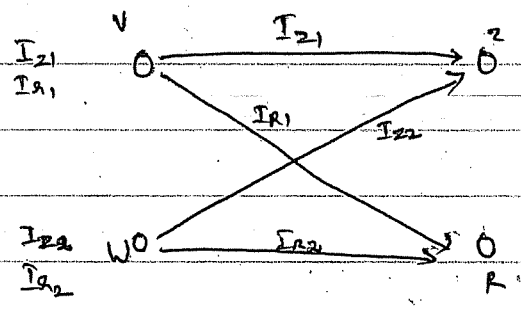
forward I_1', a_{11}, a_{12} on path 1
I_2', a_{21}, a_{22} on path 2

| only D can recover.

Anonymity → ① route set up
② data transmission.

How to do route setup?

Anonymous routes: - each nodes knows next hop
- no one else knows a node's next hop
- send next hop info in a confidential manner.



Z → I_{Z1}, I_{Z2}

R → I_{R1}, I_{R2}

Reuse nodes to send multiple pieces as long as pieces belong to different messages.

Dealing w/ churn → use n/w coding in addition to source coding.

Censor:

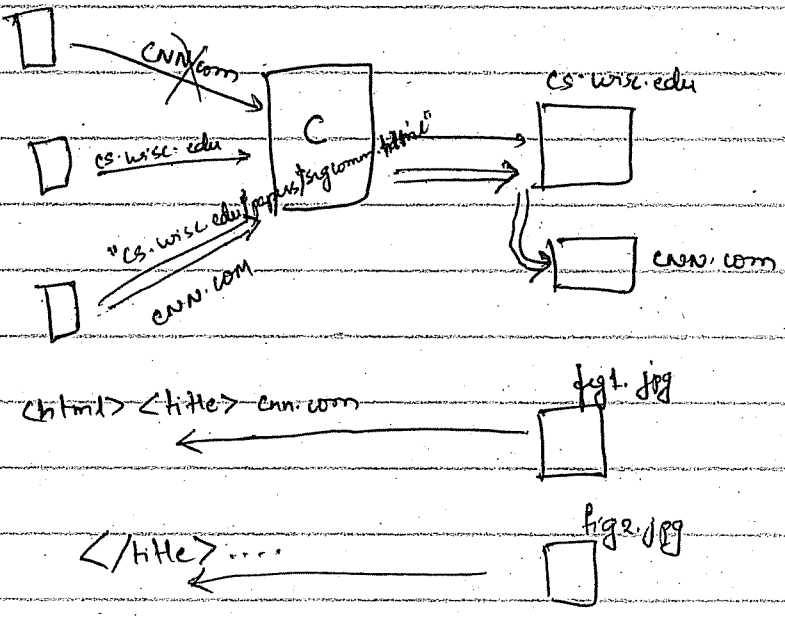
- Restrictive govt, corporate firewall.
- Discovery attacks: notice unusual looking traffic
  - suspicious web access patterns
  - use of circumvention s/w
- Disruptive attacks: block access to certain web sites
  - attempts to block access to circumvention s/w

} privacy

Design goals for censorship resistance: circumvent so that both forms of these attacks are fruitless or unsuccessful.

- deniability: can't confirm a client is accessing censored stuff
- stat den: should not arouse suspicion
- covertness for servers: can't discover a server that is serving censored content to avoid blocking.
- communication robustness: should be robust in the face of censor disruption
- reasonable performance

Big picture



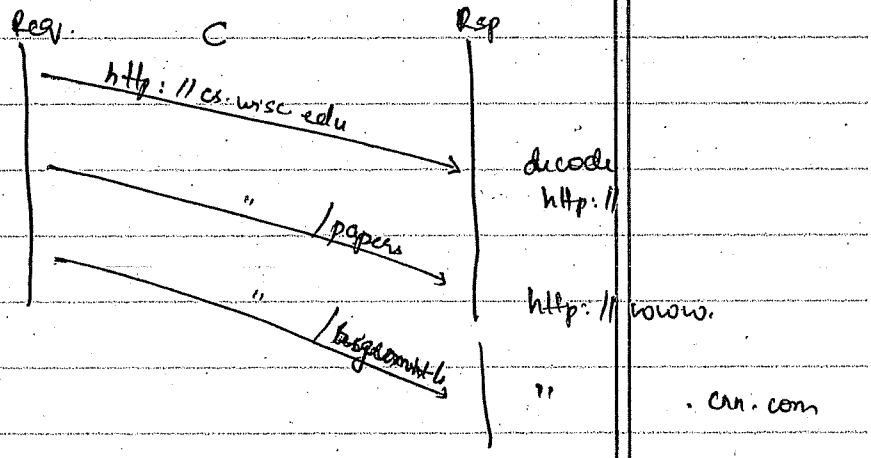
- use intranet proxy on localhost (requests)
- upstream request is sequence of messages.
- downstream response is images

Problems today

① SSL fingerprinting
② SSL looks suspicious
③ not attempt to conceal servers.
④ SSL can be blocked.

Downstream: - Embed data in the less useful portion of images.
- decided by shared secret
- need to change cover image.
↳ use a Web cam.

Upstream comm:



Mapping function: pages on responder → public pages.
↳ should be secret → critical to deniability.

Several candidates: covertness vs. bandwidth.

- Odd/even links: requester may ask for any one of half of the links
1 bit per visible http request
- Links modulo k:
any one of N/k links.
log(k) bits.
- State mapping: strange browsing → poor covertness
bandwidth M bits per request.

Range-mapping: high-bandwidth, dynamic mapping.
→ Web-surfing 20-questions style.

Assume: set of ordered URLs commonly requested.

Responder tells requester
① split strings for ranges in this set.
② mapping between split and visible requests.

Requester sends a visible http request.

Visible		Split-strings 0%	Visible		Split-strings 25%
progsells.html	→	amazon (25%)	aditya	→	cnn.
people.html		microsoft (50%)	aaron	→	ebay
publications.html		yahoo (75%)	jeff	→	java
		100%	brian.	→	microsoft-50%

This assumes that any page on the responder is equally like → NOT TRUE.