Internet Anonymity w/ Tor

Discuss: Anonymity vs Privacy vs Pseudonymity

- hide identity of person
- hide content
- IP address
- hide source of Internet traffic from websites, from traffic monitoring

Anonymizing Proxy:

Clients → Encrypted → Proxy → Website

I see user visiting this website
I see user using proxy to visit some website

Single bottleneck / point of failure
Safety in numbers
Mix-nets: eliminate single point of failure

- each relay has public key
- to connect:
  client chooses random path thru relays

Ex. \( R_1 \rightarrow R_4 \rightarrow R_2 \rightarrow R_6 \rightarrow \text{server} \)

\[ E_{\text{pk}_1}(E_{\text{pk}_2}(E_{\text{pk}_6}((\text{server, request})))) \]

Onion encryption!

\( R_2 \) sees encryption of \( R_6 \), cipher text from \( R_4 \)

\( \Rightarrow \) relays know only prev. / next hop

Problem: very expensive \( \Rightarrow \) high latency

how does server respond?

- relays can retrace route \( \Rightarrow \) keep state
  or send "return address" onion
Watermarking attack:

... \( \rightarrow (R_i) \rightarrow (R_1) \rightarrow (R_{i2}) \rightarrow ... \)

\( R_i \) & \( R_{i2} \) are malicious

\( \rightarrow \) coordinate to agree on a seq. of numbers \( d_1, d_2, ... \)

\( R_i \) introduce artificial delays of \( d_1, ... \)

\( R_{i2} \) can try to detect signal \( \Rightarrow \) associate different msgs in mix-net w/ same connection

**Tor:** attempt to tradeoff between 2 solutions

- generate "circuits" through the network
  - setup circuit using pub key crypto
  - use circuit using symm key crypto
  - generate circuits in background.
Diffie-Hellman key agreement

Client → DHKA → R₁
agree on shared key $K₁$

use $K₁$ as an AES key

$C \xrightarrow{DHKA} R₂$

$E_{K₁}(R₂)$