CS-438
Decentralized Systems Engineering

Fall 2021

Week 11

Anonymous communication

Motivations:

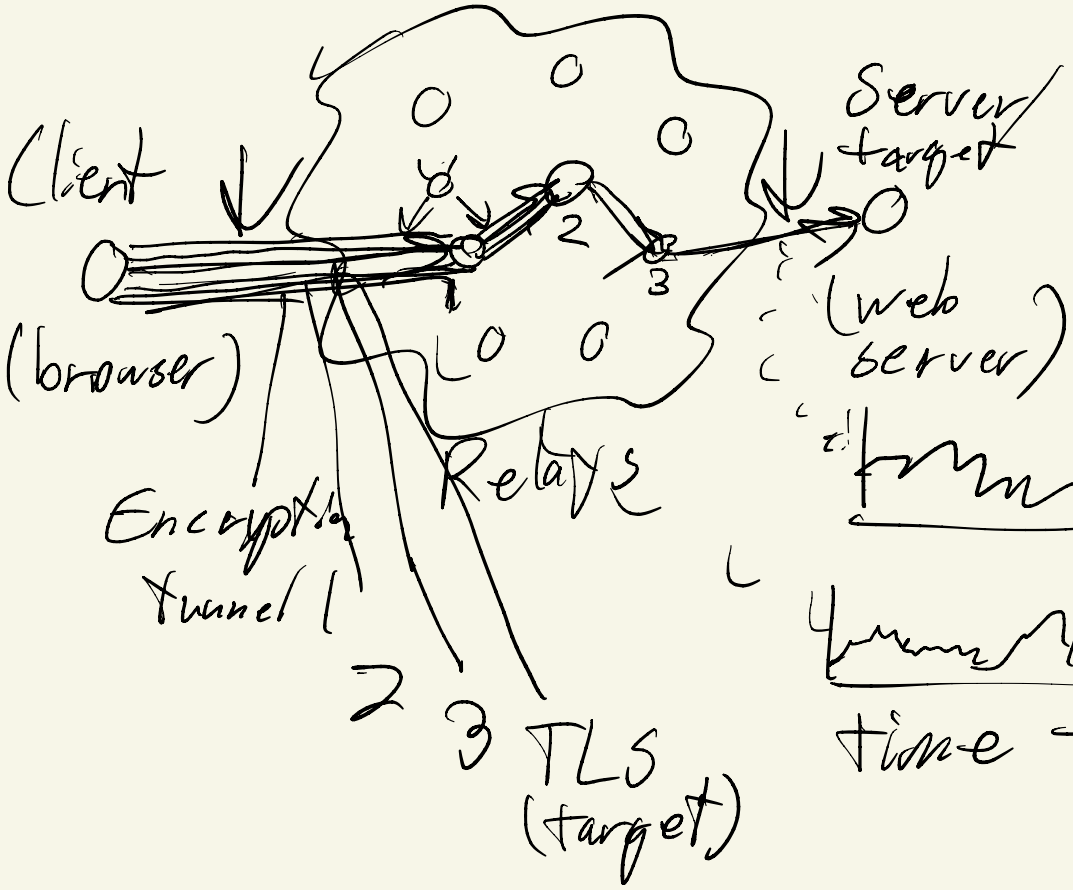
- Basic right to privacy - for metadata (not just data)
  - metadata reveals "a lot" - correlated, tracked
- evade geographic restrictions
- hide associations, relationships, activities
- get past "great firewalls" - censorship
- hidden services - The Dark Web™
- journalists, public figures, celebrities, privacy-conscious, criminals, dissidents, spies, police, honeypots, whistleblowers
- voting - freedom of expression

Approaches:

- disable active content "say no" to cookies, Do Not Track header
- dynamic IP, NAT, shared computer, randomized MAC addresses, public cloud, phone numbers (WhatsApp, Signal...)
  - usually associated with identity
- VPNs – Apple Private Relay
  - single-hop relay
  - glorified proxies
  - Tor – 3-hop relay
  - 2-hop relay

  } relaying – MIX nets (Chaum, 81?)
- Dining Cryptographers – information coding) (Chaum, 88?)

Tor – The Onion Router



- 256-byte cells
  512?

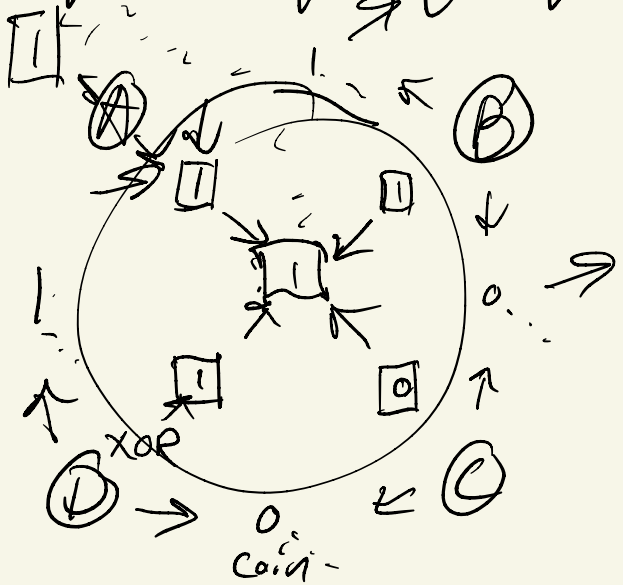
Properties:

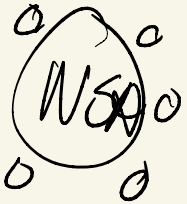
- strong against local adversary
- weakness to correlation (timing)

mitigations:

- adding delays (Mix nets)
- batching

Dining cryptographers (DC-nets) – Chaum





ring shaking topology

- provable, information-theoretic, "perfect" anonymity
- "anononymity set"
- parallelizable (PriFi – low-latency DC-net)

Misbehavior

- anonymity set excludes colluding nodes
- 2 misbehaving nodes: (ring topology): can split ring
  - more connected sharing topology:
    - complete graph: all-to-all
    - random "degree" graph – w.h.p.
    - (Dissent, Verdict) – all clients to all servers