CS-234
Technologies for Democratic society

Fall 2021

Week 12

Technologies / approaches for identity

Weak proxies:

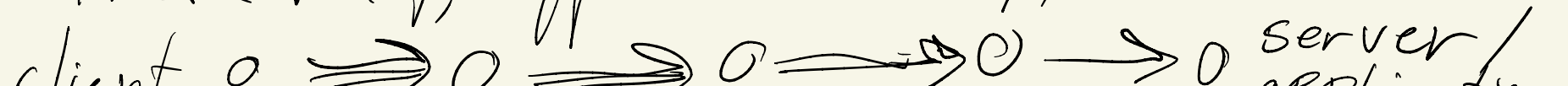
- self-declared identities/accounts - no verification
  - users: choices, inclusion
  - providers: simple, low overhead, low risk, low barrier to acquire users
- delegated social media/ single-sign-on ("login with X")
  - users: reuse existing account, less form-filling "1 click", reduced disclosure
  - providers: simpler, building on standard framework/APIs
    - centralized, exclusionary
    - more centralized data collection, tracking
    - no password DB, other risky PII
- IP addrs, email addrs, mobile phone #s
- "Turing tests" - CAPTCHAs - "identify as a person"
  - rate-limit abuse

Stronger identity technologies

- Institution / government single sign-on (SSO): EPFL, SwissID
  - verified government-issued documents
  - online verification ("Know Your Customer")
    - financial services
    - scan of passport, send selfie, scan chip
      freshness proof (today's newspaper), utility bill (proof of address)
    - video sessions - "liveness tests" (AI/ML)
- PKI (x.509), PGP "Web of Trust", Namecoin, ENS, ...
- Biometric identity - Aadhaar, Worldcoin
  registration: scan biometrics (2 eyes + 10 fingers)
  incorporates into database, deduplicates (1-to-many comparison)
- Self-sovereign identity: "more decentralized SSO"

Technologies/approaches for anonymity

- Anonymous communication/interaction (Speakup, Onion routing (Tor), Firefox Relay, Apple Private Relay, VPNs)



Dining Cryptographers (DC-nets) - Chaum '88

- Anonymous identity?
  - Randomised MAC addresses
  - ...