CS-438 Decentralized Systems Engineering

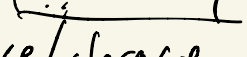
Week 9

Sybil attacks and defenses, permissionless consensus

"The Sybil Attack" - Douceur

- fake identities - virtual nodes, social bots, sockpuppets, astroturfing, fake reviews, ballot stuffing

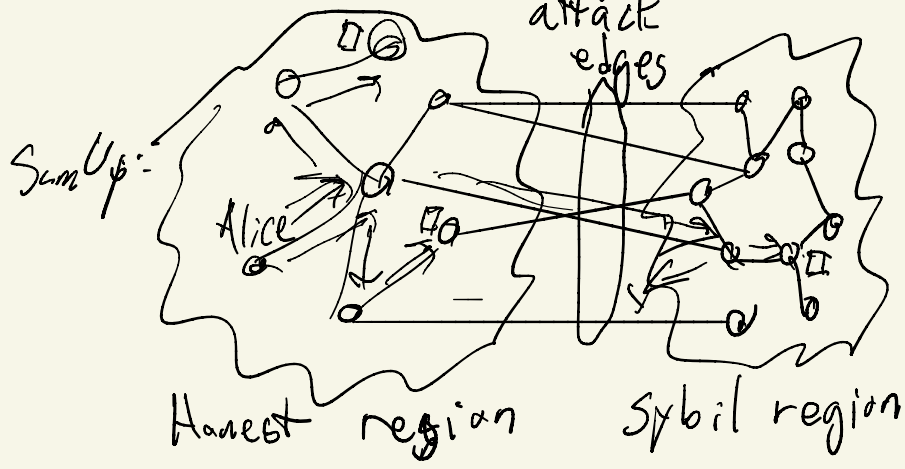
Defenses:

- Strong identity (PKI): ID verification (KYC) ("know your customer"), biometrics (face, fingerprints, iris, ...)
  - Aadhaar (India)
  - Weaknesses: privacy - need centralized database, uniqueness test: ∀existing IDs, check new ID ≠ that
  - Forgeability, synthesis of biometrics
- Artificial cost: proof-of-work (crypto puzzles), threshold validation, time delay, digital credit/"stake" - proof of stake
  (block, counter) → H → 

  proof of space/storage, CAPTCHA (Turing tests)
- Social network
- Proof of personhood

Social / Trust Network defenses

- PGP "Web of Trust" model: "Alice" ⇒ K_A "Bob" ⇒ K_B (alternative to PKI)
  - S&L/TLS PKI – only widespread for websites, not client-side certs, E-mail address validation PKI (Email challenge)
    Not Sybil-resistant: alice@gmail.com ⇒ alice+abc@gmail
  - Keybase – mainly PKI / naming
- Research:
  - Generic: SybilGuard, SybilLimit, SybilRank, ---
    App-specific: SumUp (recommendations), Whānau (DHT)[6], dSybil
- Assume social graph, edges denote "trust", "Sybil region" Scenario;
  - honest region "well-connected"
  - attack edges are costly, relatively rare/few
  - Bound the effective "power" of Sybil nodes



Weaknesses: – Privacy
- Bruce Schneier – "movie plot" threats
- Alternatives: crowdsourcing, sparse infiltration, small-scale attack → raising $ costs

Proof of personhood

Goals:

- Inclusion: low cost participation to anyone (permissionless)
- Equality: "one person, one vote" - strict
- Security: against Sybil attacks, identity loss/theft
- Privacy: no ID / biometrics, databases, ...

Pseudonym parties, Encointer, Idena, BrightID, Upala, GoodDollar, ...