CS-234
Technologies for Democratic society

Fall 2022

Week 10

Sybil attacks

Internet has only "weak" identities
- IP address
- user accounts / profiles

One user could create/control many accounts
- voting: ballot-stuffing
- DDoS?
- spam - against email, online forums
- threshold secure algorithms - consensus

"Good"/Legit reasons for multiple accounts

Privacy — discuss sensitive issues w/o fear
- creepy tracking detection
- separating professional & personal/private roles

Topic/purpose specialization

Sybil defenses

Cost-centric vs human-centric

- Charge fees (membership, etc)
- Smart contracts: staking & slashing
- Verifiable identity proxies
  - phone # - WhatsApp
- Membership referral requirements
- CAPTCHA - cost in human time + annoyance

Defenses - human-centric "one per person"

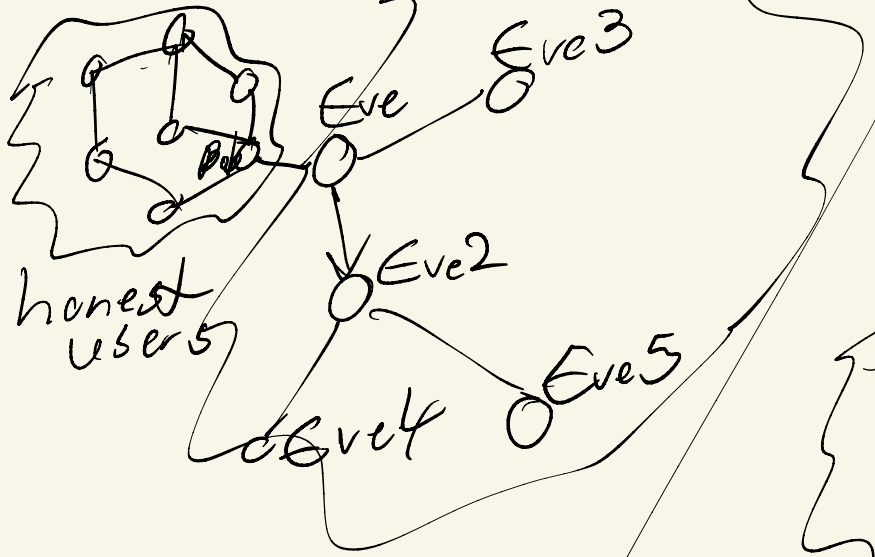
Strong identity checking - KYC
"Know your customer"
Cost/deterrent: false paper trail, police...

Reputation-based
Based on usage history
Social reputation / trust networks
early precedent: PGP "pretty good privacy"
Cryptocurrency/blockchain: Kleros, HumanityDAO, Idena...

(to be continued...

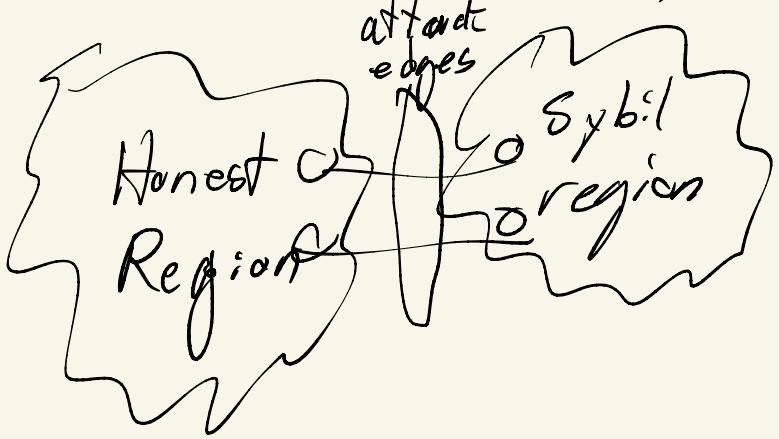
trust-network approaches

problem:



graph-based Sybil defenses:

SybilLimit, SumUp, Whanau, trustRank, ...



... Continued

Biometric identity
- India - Aadhaar
- World food program
- WorldCoin

Presence - based - pseudonym parties
- Encointer (Zurich)
- Idena (Online presence tests)