CS-234
Technologies for Democratic society

Fall 2022

Week 12

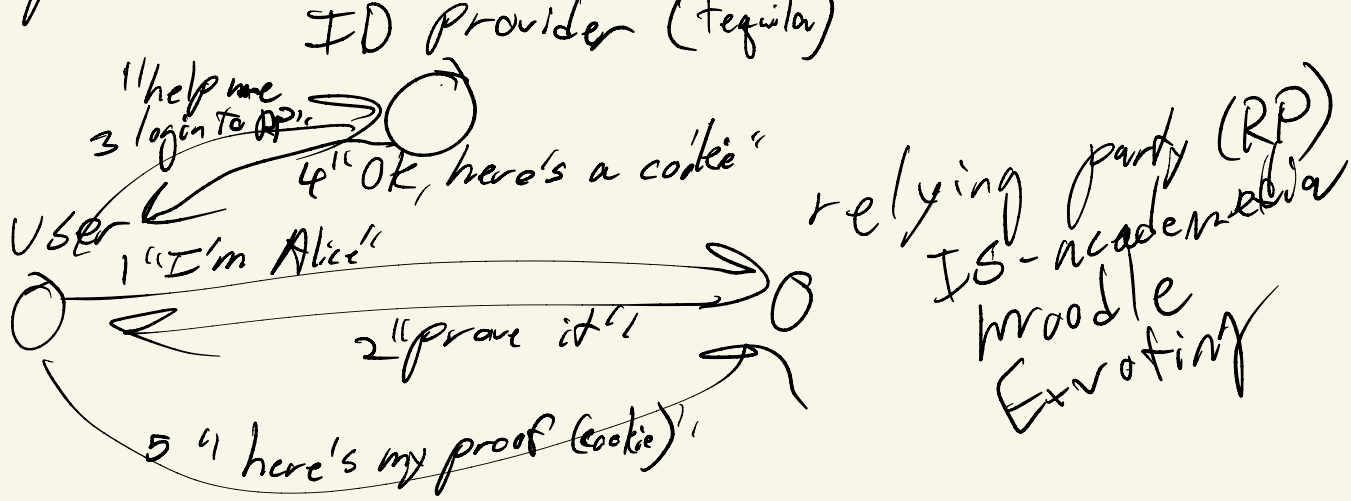
Identity & anonymity technologies

Identity technologies

- government ID
  - digital checking of legacy IDs (KYC)
- federated identity
- e-ID, (Estonia, ...)
  e.g. Swiss ~~EID~~ referendum
- self-sovereign ID

Federated ID (tequila / GASPAR)

- Inspiration: Kerberos - MIT



- Social platforms:
  "Login with: Google, Facebook, Twitter, ..."

Identity properties to be proven:

- membership in certain group (students, faculty, staff, ...)
- continuity - same user, for state persistence
  associate state w/ user
- uniqueness - one per user (E-voting)
- authenticity of user - is the intended user
- prove age for adult websites, ordering liquor, ...
- prove citizenship, status
- prove credentials (EPFL degree, ...)

Privacy-preserving mechanisms

- privacy wrt whom?
  who do you trust with how much info?
- minimize information disclosure: eg. RP learns only that age ≥ T
- prove $\sum$age ≥ T_{vaud}, live in Vaud?
- better: "proof of adulthood" (hiding both age & locality)
  - anonymous credentials
- SSI: most use-cases proving properties of ID
  most are not "interesting" (to RP) w/o many others
  only few ID properties uniquely identify a person

Online services

- eg. Netflix cares about:
  - if you'll pay
  - what you're allowed to watch (age)
  - what you're license to watch (region)
  - what your interests are
    - what you're watching, have watched
  - what to recommend to you
    to others

based on info from many users

buy/sell user data

Promising privacy-preserving techniques:

- Private/anonymous recommender/reputation systems (e.g. AnonRep)
- Privacy-preserving ad systems
- Privacy-preserving federated machine learning (eg. LDS / TuneInsight)