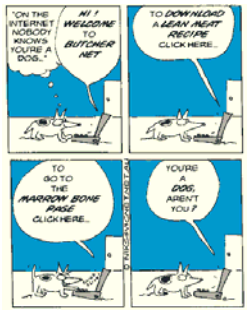
The Privacy Problem

Prof. Bart Preneel
COSIC
Katholieke Universiteit Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel
September 2010

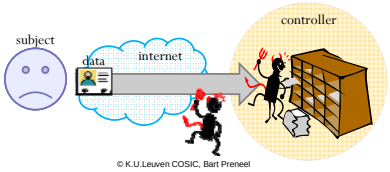
A picture is worth more than a thousand words

"On the Internet, nobody knows you're a dog."
New Yorker, 1993



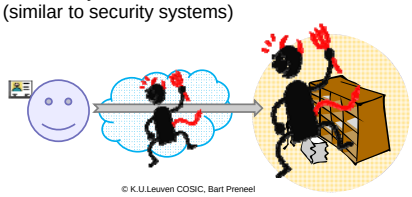
Soft privacy

- system model
  - data subject provides her data
  - data controller responsible for its protection
- threat model
  - external parties, errors, malicious insider



Hard privacy

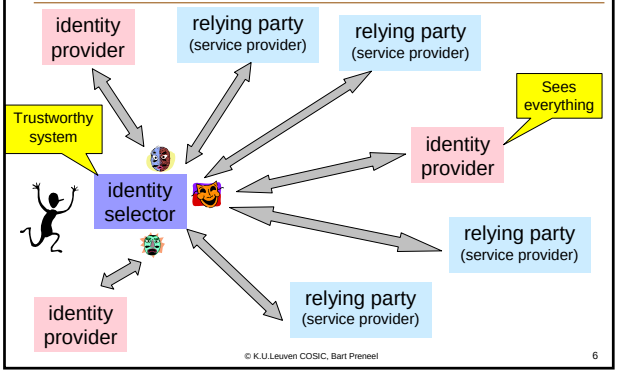
- system model
  - subject provides as little data as possible
- reduce as much as possible the need to "trust" other entities
- threat model
  - adversarial environment: communication provider, data holder
  - strategic adversary with certain resources motivated to breach privacy (similar to security systems)



The great thing about identity management standards is……there are so many to choose from!

kantara INITIATIVE
ICAM
Google
OpenID
myspaceID.
OAUTH
WS-Federation
OASIS
OIX OPEN IDENTITY EXCHANGE
LIBERTY ALLIANCE PROJECT

Identity meta-system: "user-centric"



Identity management

Are users capable and qualified to manage their own identities?
Do they understand the implications?

User

Centralization allows data mining
Results in personalization recommendation systems, fraud management

Identity provider for e-gov
Identity provider for society
Timescales

Business

Government

Technology

- on-line versus off-line
- centralization versus distributed
  - privacy risk
  - singe point of failure
  - ease of use
  - monetization
- reputation-based systems
- threshold systems (distributed identity)
- anonymous credentials
- biometrics?





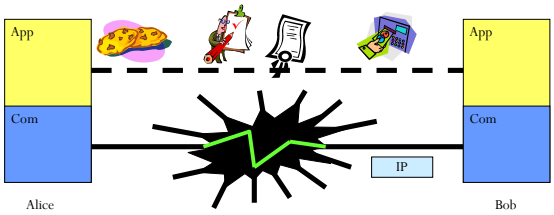
Anonymous credentials [Chaum'85]



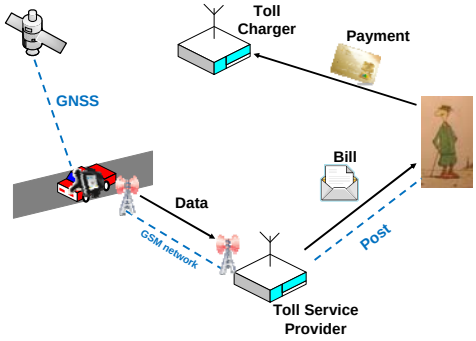

Anonymous Credentials

Anonymous communications

- Applications assume that the **communication** channels are secured / maintain privacy properties
  - previous protocols are useless if the adversary can link transactions based on traffic data (e.g., IP/MAC address, IMEI, GPS, browser: https://panopticlick.eff.org/)

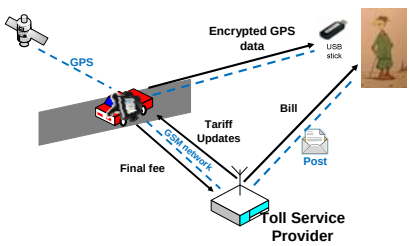


Road pricing: straightforward implementation



Privacy-Friendly Electronic Toll Pricing

No personal data leaves the domain of the user



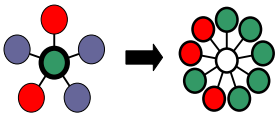
J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," *19th USENIX Security Symposium 2010*, 2010.
https://www.cosic.esat.kuleuven.be/publications/article-1408.pdf

Advanced protocols: now practical

- multi-party computation
- threshold crypto
- privacy protecting data mining
- social and group crypto

decryption based on location and context

distance bounding



"you can trust it because you don't have to"