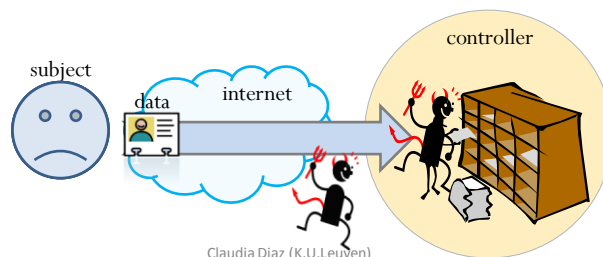


Privacy Enhancing Technologies

Claudia Diaz
K.U.Leuven ESAT/COSIC

“Trust-based” or “Soft” privacy

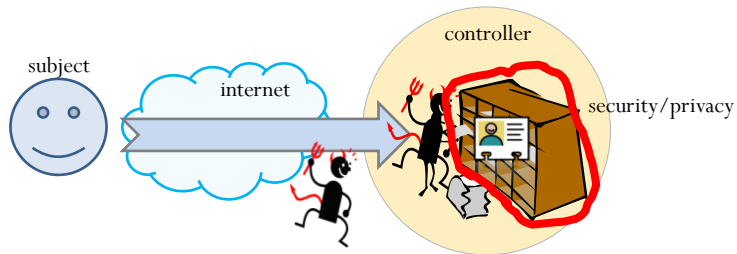
- System model: data protection oriented
 - Data subject provides her data
 - Data controller responsible for its protection
- Threat model
 - External parties, errors, malicious insider



2

Soft privacy

- Controller: main security “user”
- Policies, access control, trust, audits (liability)
- Goal (data protection): purpose, consent, data security

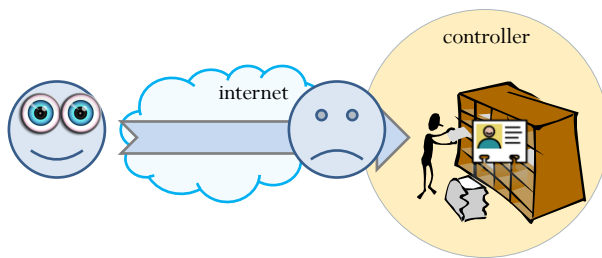


Claudia Diaz (K.U.Leuven)

3

Soft privacy

- Data subject has already lost control of her data
 - In practice, very difficult for data subject to verify how her data is collected and processed

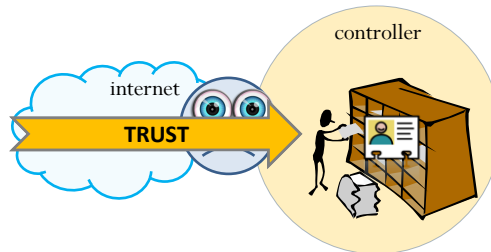


Claudia Diaz (K.U.Leuven)

4

Soft privacy

- Data subject has already lost control of her data
 - In practice, very difficult for data subject to verify how her data is collected and processed
 - “Need to trust” data controllers (honesty, competence) and hope for the best
 - Weak enforcement, low penalties



Claudia Diaz (K.U.Leuven)

TRUST ASSUMPTIONS?

INCENTIVES?

TECHNOLOGICALLY
ENFORCED?

5

Privacy = Security Property

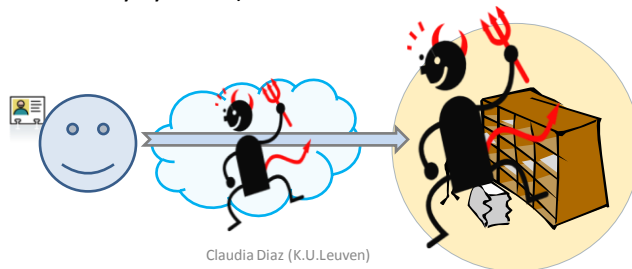
- Governments / Military
 - Protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations
- Companies
 - Protection of trade secrets, business strategy, internal operations, access to patents
- Individuals
 - Freedom from intrusion, profiling and manipulation, protection against crime / identity theft, control over one's information
- Shared infrastructure
 - Despite varying capabilities infrastructure is shared
 - Telecommunications, operating systems, search engines, on-line shops, software...
 - **Denying security to some, means denying it to all !**

Claudia Diaz (K.U.Leuven)

6

Hard privacy

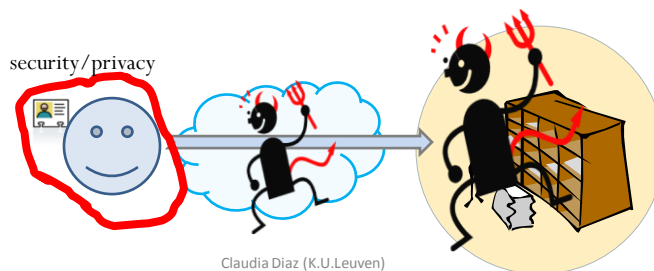
- System model
 - Subject discloses as little data as possible
- Reduce as much as possible the need to “trust” other entities
- Threat model
 - Adversarial environment: communication provider, data holder
 - Strategic adversary with certain resources motivated to breach privacy (similar to security systems)



7

Hard privacy

- Subject is an active security “user”
- Goal (data protection): data minimization (trust minimization)
- Technologies:
 - **Solutions based on anonymity/hiding identity:** anonymous communications, anonymous credential protocols, anonymous e-cash
 - **Solutions based on hiding actions/data/content:** oblivious transfer, commitments, private information retrieval, keep user data at user side



8

Two main approaches

- Anonymity
 - Service provider can observe access to the service
 - Cannot observe the identity of the user
- Oblivious Transfer (OT) / Private Information Retrieval (PIR)
 - Service provider can identify user
 - Cannot observe details of the access to the service
 - Which records were accessed
 - Which search keywords were used
 - Which content was downloaded
 - ...
- All parties have assurance that the other participants in the protocol are cannot cheat

Claudia Diaz (K.U.Leuven)

9

Examples of Technologies

- Anonymous communications
 - 3rd party anonymity: email, instant messaging
 - Recipient anonymity: web browsing
- Anonymous authentication
 - Verified attributes
- Private information retrieval
 - Protect access patterns
- Private keyword search
 - Protect keywords as well as results
- PriPAYD, PrETP
 - Conceal location data, while ensuring the correctness and integrity of payments
- Privacy-preserving smart metering
 - Conceal energy consumption data, while ensuring the correctness and integrity of payments

Conclusion

- Soft privacy:
 - give all your data, trust provider
 - provider builds big database
 - you pray
 - hidden costs? who bears the impact of a privacy breach?
- Hard privacy
 - use advanced privacy technologies to implement functionalities while revealing minimal data
 - if provider is evil / compromised, the impact of breach is much less serious