Engineering Privacy by Design

Claudia Diaz
KU Leuven / COSIC

PRIPARE – Athens, May 2014

Context

- Implementing privacy in systems is difficult
  - privacy requirements must be integrated in systems engineering activities
- Few existing systems designed with robust privacy protection in mind
- The term “Privacy by Design” is widely used by policy makers
  - IPC Ontario: 7 principles
  - EU Commissions Communication: “A comprehensive strategy on data protection in the European Union”
  - FTC report: “Protecting consumer privacy in an era of rapid change”
- What do PbD principles say to engineers developing systems?

Engineering perspective

- Disconnect between policy makers and engineers on what it means to technically address privacy threats

- "Control" and "transparency" do not mitigate the privacy risks that arise from mass collection of data in databases
  - Single point of failure
  - Attractive target
  - Hard to secure (SP itself / malicious insiders / accidental disclosure / outsiders)
  - Risks of public disclosure, and/or "stealthy" abuses (e.g., secondary use)

Properties of digital systems

- Properties of digital systems:
  - Easy to replicate and distribute digital information
  - Statistical inferences, linkability across contexts
  - Computational capabilities: more can be done with less data

- Not "just" with our understanding of what data minimization may mean in the analogue world
  - Lack of metaphors / intuition to explain "magical" capabilities (eg, ZK protocols)

- Data minimization principle
  - The principle can be taken **much** further than what would usually be considered to be "adequate, relevant and not excessive in relation to the purpose"

Techniques for data minimization

- Anonymity
  - Service provider can observe access to the service
  - Cannot observe the identity of the user
  - Robust anonymization is difficult: multiple layers
  - Understanding anonymity sets not trivial

- Oblivious Transfer (OT) / Private Information Retrieval (PIR)
  - Service provider can identify user
  - Cannot observe details of the access to the service
  - How to convey the technical intuition to non-experts?

Towards PbD methodology

- Functional requirements analysis
  - It is critical to provide a precise description of what the system should do
- Data minimization (several dimensions)
  - Find the minimum set of data that is strictly necessary to fulfill the functionality, and the integrity of the system
  - Data may reside in the system but in the user device instead of in centralized database
  - Anonymity / Advanced crypto protocols / both: requires knowledge of the state of the art in privacy technologies
- Modeling attackers, threats, and risks
  - Some threats (eg, secondary use, inferences, abuse derived from *authorized* access) may not be obvious to non-privacy-expert systems designers
- Multilateral Security Requirements Analysis: security requirements of the different stakeholders (eg, integrity)
- Implementation and testing of the design (re-iteration and re-evaluation of risks and threats)

Other considerations

- Ethical, legal and political analysis of proportionality
  - "Legitimacy" of the desired system given its burden on privacy: "the establishment that the application goals would be useful for the intended use population"

- Privacy by design and population surveillance
  - If the purpose of the system is to do intrusive surveillance of populations, then putting a privacy by design label on these systems is misleading (white-washing of intrusive systems)

- Risks and social norms
  - Non-technical risks (e.g., discrimination of populations)

Take away points

- Data minimization must have a central role for PbD
- Data minimization not only about anonymity
- Need for better intuition / metaphors to convey to non-experts what state-of-the-art privacy technologies can do
  - Specific expertise is needed
- Need to deploy robust privacy systems that can be used as a reference
- Need for engineering methodologies for PbD
  - Avoid reducing PbD to checklists that can be easily ticked away for compliance