Privacy and Data Protection 4 Engineering

Addressing the stakes of data protection from systems specifications to software

2019/05/17
Stakes Of Privacy And Data Protection In A Nutshell

Image borrowed from https://www.digitalvidya.com/
Stakes Of Privacy And Data Protection In A Nutshell

Former background
- Networked, distributed applications, and storage
- Almost no enforcing policy nor rules for business or industry
- Almost no obligation for stakeholders
- Almost no rights for individuals

Transition factors
- Growing markets and business based upon data
- Growing usage of information related to individuals
- Increasing computing power (HW)
- Inference algorithms (Data mining, Artificial Intelligence)
- Emerging regulations

Evolution stakes
- Keep a suitable balance between needs
- Keep compliance with regulations
- Support stakeholders in the process (lawyers, engineers, developers)
- Generate evidence of systems’ properties (compliance, trustiness)
Categories Of Concerns And Impacts

**Accident de tramway à Issy-les-Moulineaux : les travaux vont prendre plusieurs jours**

**Altran, géant français du conseil en technologie, victime d’une cyberattaque**

Altran a assuré que l’attaque n’avait donné lieu à « aucun vol de données » ni « aucun cas de propagation de l’incident à des clients ».

**Airbus a détecté un « incident de cybersécurité » dans sa division d’avions commerciaux**

Cette intrusion a « entrainé un accès non autorisé aux données de l’entreprise », affirme Airbus, mais n’a eu « aucun impact » sur ses opérations commerciales.
STANDARDS AND REGULATIONS

- General Data Protection Regulation (GDPR)
- Technical international standards:
  - ISO 29100: Privacy framework
  - ISO 27550: Privacy engineering
  - ISO 27552: Requirements and guidelines

METHODS TO ACHIEVE PRIVACY & DATA PROTECTION by design

- PROPAN: for requirements elicitation
- PRIPARE: for iterative (agile) design
- LINDDUN: design guided by risks

ALGORITHMS, TECHNIQUES FOR PRIVACY & DATA PROTECTION

- Minimization
- Fragmentation
- Pseudonymisation
- Analysis of architectural models and transformation
Proposals and Positioning

Scheme of the proposed solutions and positioning w.r.t. typical SDLC.

1. Identify violated/concerned reqs.
   1.1. Identify violated/concerned properties

2. Trace concerned reqs. to the architecture
   2.1. Improve architectural elements

3. Implement architectural improvements
   3.1. Adapt code

4. Trace and validate properties
   4.1. Verify code

5. Propagate results to requirements

Formal Framework For Privacy Related Properties Verification

- **Formal languages and semantics for:**
  - **Systems modeling:**
    - Data flows
    - Stakeholders
    - Storage units
    - Processing units
  - **Expressing properties to verify:**
    - Unlinkability, Unidentifiability, Repudiation, Undetectability, Undisclosure of information, Awareness, Compliance
  - **Conducting verification of properties:**
    - Semantics
    - Algorithms
  - **For executable parts of systems:**
    - Verification of properties on code
    - Extension of Frama-C
    - Extension of SecureFlow

Developed in the scope of a PhD (J. Signoles, G. Pedroza, T. Antignac)
1. Methods and tools for Privacy-by-design
2. Leverage existent knowhow on data protection for engineers
3. Spread the adoption of data protection practice in time and space
4. Demonstrate readiness for GDPR compliance: pilots for the automotive and smart grid domains

https://www.pdp4e-project.eu/
PDP4E Work Packages

WP1: Project management and governance

WP2: Specification and architecture of methods and tools for Data Protection Engineering

WP7: Validation, demonstration and exploitation

WP3: Methods and tools for data protection risk management

Development of methods and tools for Data Protection Engineering

WP4: Methods and tools for data protection requirement engineering

WP5: Methods and tools for data protection model-driven design

WP6: Methods and tools for data protection assurance

WP8: Dissemination, communication and liaison
Methods and Tools for GDPR Compliance through Privacy and Data Protection for Engineering

For more information, visit: www.pdp4e-project.org

Thank you for your attention

Questions?

gabriel.pedroza@cea.fr