SECENTIS

A European Industrial Doctorate on Security and Trust

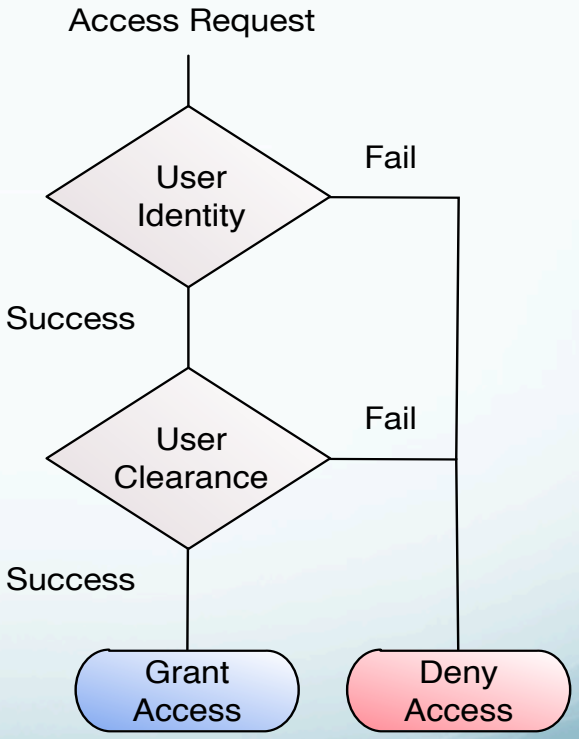
Risk-Based Access Control

Nadia METOUI
Alessandro ARMANDO (FBK Advisor)
Michele BEZZI (SAP Advisor)

21st October 2014

Traditional Approaches

- Rely Hard coded Authorizations predefined by the Security Administrator of the Resource Owner.
- The Decision Logic is based on Attribute comparison.
- The Risk is not explicitly considered and No Exceptions are made



Traditional Access Decision Logic

New Challenges

- Organizations want to increase access to the data… but:
  - To protect sensitive information (e.g., PII).
  - To preserve a High Compliance Level and manage Risk
  - To reduce Cost and improve Operational Efficiency
- Challenges
  - Align with both business objectives and the risk landscape
  - Adapt with new concepts and technologies

Mobile Devices and BYOD

Cloud Computing

Social Networks

Risk Aware Approaches

- Risk Aware Approaches aim to provide flexible access control decisions and more efficient risk management.

- Risk in Risk Aware AC models is a function of:
  - Likelihood of a permission misuse
  - Cost of this misuse

- Risk mitigation Strategies are applied to lower the impact of eventual misuse
  - pre-obligations
  - post-obligations

Privacy in RAAC

- Risk-aware access control has received a growing attention in the last few years
- Little attention is given privacy aspects of risk-aware access control
- Preserving privacy by enforcing privacy policy on top of the access control evaluation process

Case Study: Sensitive Information Disclosure

Businesses create consume Data

Data Monetization Businesses

Sensitive and Private

Strict Regulations

complex, costly, and risky to handle

The Problem

- When dealing with privacy-sensitive data:
  - Drastic all-or-nothing access decision methods
  - The accepted risk level is statically given.
- The accepted risk level may depend on a number of factors that can only be computed at run-time (i.e. dynamically):
  - User Trustworthiness or Competence
  - Security Context etc.
- **Need:** develop new access control model that
  - provides the largest possible amount of information,
  - while preserving anonymity

Approach

- Quantify the disclosure risk associated with the query and compare it with the "acceptable" risk threshold.

- If the threshold is exceeded, apply anonymization techniques to dynamically reduce the risk below the threshold.

- This operations dose not yield the exact data set the user asked for but:
  - Provide relevant information to the user
  - Preserves anonymity according to some pre-defined disclosure-risk levels.

Information Disclosure

- Data attributes (Columns) in a database can be classified as follows.
  - Identifiers
  - Quasi-identifiers (QIs)
  - Sensitive attributes

- Disclosure Risk
  - the probability of Re-identifying individuals
  - the harm caused by the misuse or abuse of their sensitive information.

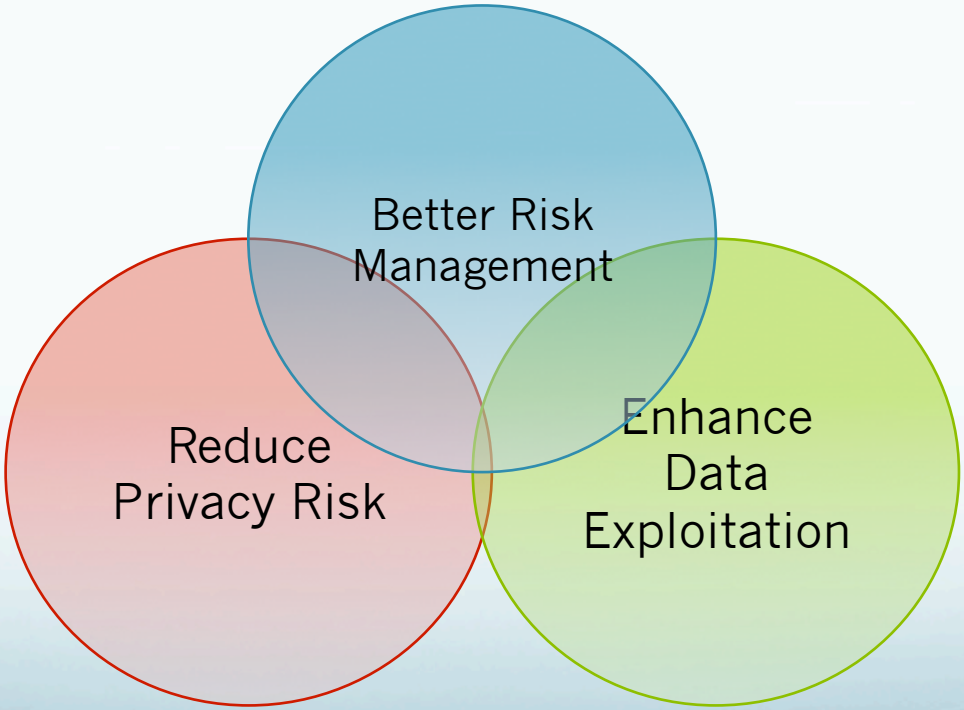
Privacy Preserving

- Privacy metrics provide a quantitative assessment of the different risks associated to data release
  - k-anonymity
  - l-diversity
  - t-closeness

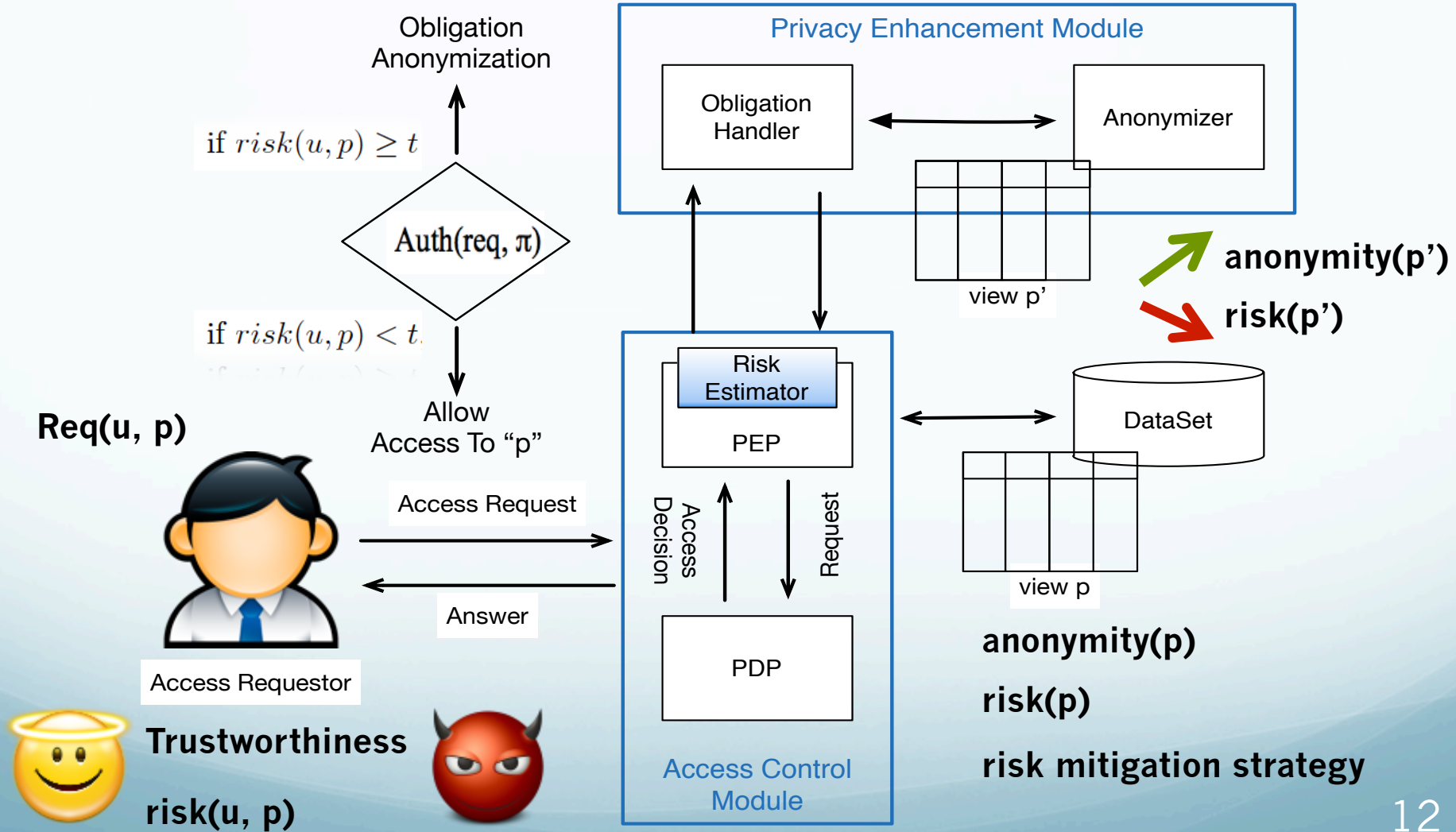
- Anonymization Operations
  - Obfuscation
  - Adding noise
  - Generalization

Proposed Solution

- Run time anonymization model
  - Evaluate Privacy Risk for each Access Request
  - Use adaptive anonymization operations as risk-mitigation methods



Risk-Aware Information Disclosure Model



Real Life Scenarios

- Satisfaction Surveys (Employee Survey)
- Healthcare (Real time monitoring)
- Discrimination prevention

Conclusion

- In our model decisions are based on the privacy risk associated with a data access request.
- Anonymization operations are used as risk-mitigation methods to satisfy an acceptable level of risk.
- Pre-obligation are used to enforce the anonimisation operations
- This allows us to return anonymized responses that are privacy preserving instead of systematically rejecting problematic requests.

Future Work

- Implementing the risk-aware information disclosure framework
- Assessing the framework against a real-world dataset

Thank you !
Any Questions ?

metoui@fbk.eu