Session 1 Report: Privacy Preserving Cloud Applications

Presenters:

Pascal Felber & Sonia Ben Mokhtar

Reporter: Bojan Cukic
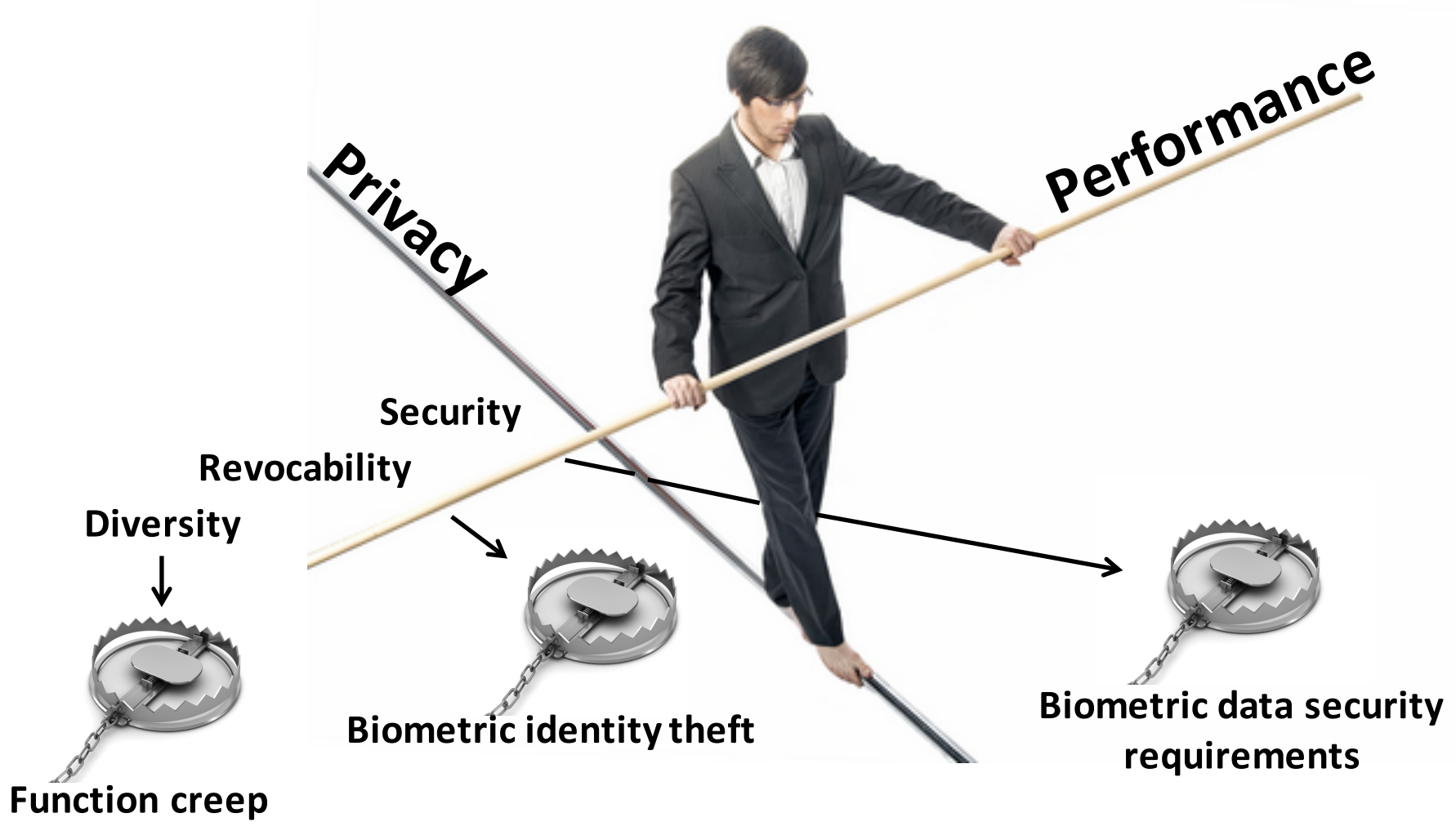
Trusted Execution Environments and Privacy-preserving Cloud Applications

- Presented by Pascal

- Discussed importance for protecting data in clouds

  – Protecting providers against malicious cloud tenants

  – Protecting tenants against provider's insider threats and platform deficiencies

- Protected mode execution insufficient, homomorphic encryption not scalable

- Intel SGX (software guard extension), enclaves

  – TEEs like SGX provide a first practical solution that combines efficiency and security

Enforcing Privacy in On-line Services (the privacy – utility tradeoff)

- Presented by Sonia

- Privacy threats from data collected by search / location / etc. service providers.

  – Collected data shared or sold

- Existing solutions: limited data sharing

  – Typically impacts utility

- Emerging solutions: application – specific "obfuscation"

  – Geo-indistinguishability

- How to measure privacy? Utility?

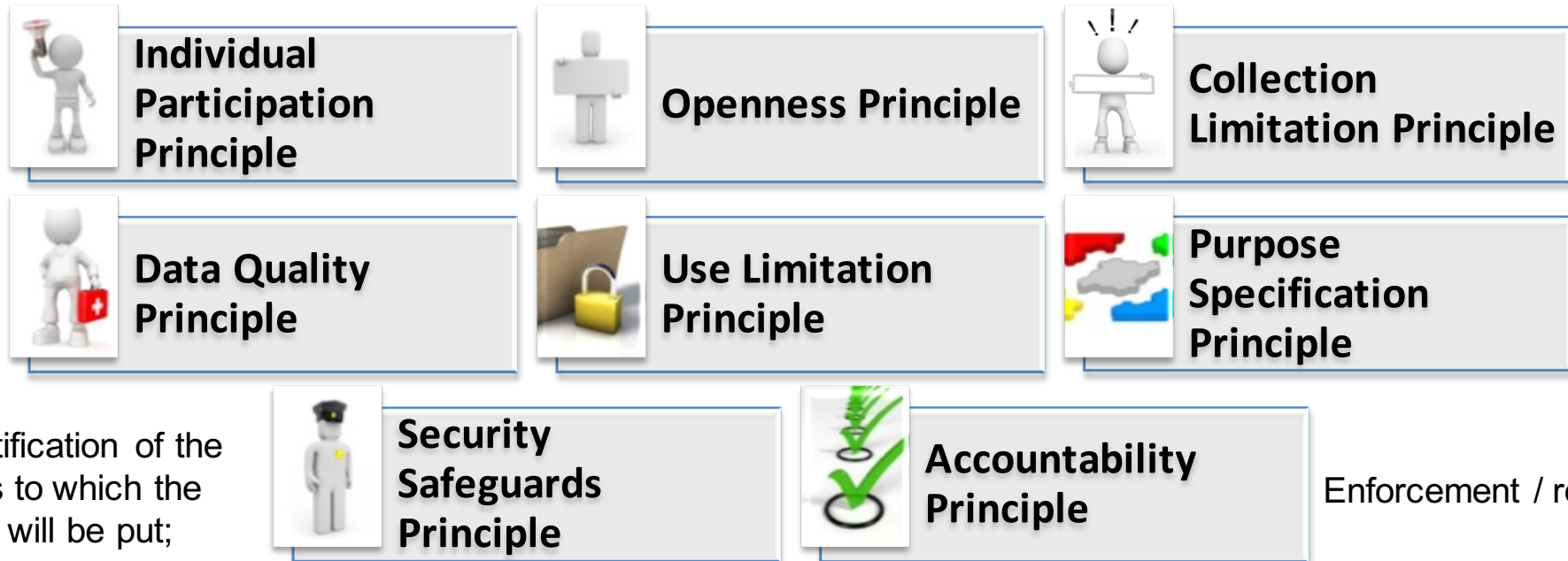 – Metrics and measures typically not generalizable

Identity Protection in IdM

Privacy

Performance

Security

Revocability

Diversity

Function creep

Biometric identity theft

Biometric data security requirements

Privacy Protection Principles

- OECD's fair information practices (FIPs) are foundational privacy protection principles.

whether the provision of the requested data is voluntary or required

identification of the entity collecting the data

Choice/Consent

Access/Participation

identification of any potential recipients of the data

the nature of the data collected and the means by which it is collected

Individual Participation Principle

Openness Principle

Collection Limitation Principle

Data Quality Principle

Use Limitation Principle

Purpose Specification Principle

identification of the uses to which the data will be put;

Security Safeguards Principle

Accountability Principle

Enforcement / redress

steps taken by the data collector to ensure the confidentiality, integrity and quality

reserved.

Version 2.0

Some thoughts on IFIP WG 10.4 role

- Definitions of privacy in computing generally lacking

- Significant gap between socio-economic definitions and technical needs

  - Security and privacy research did not make strides towards practical measurement

- This may be opportunity for WG 10.4 to offer significant contribution!