Employing Trusted Computing for Privacy-Aware Business-Processes

Ammar Alkassar

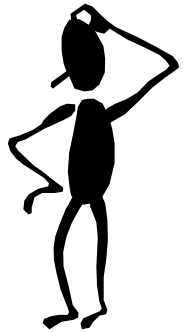
Identity and Business Models

Motivation:

Motivating Example: Travel Agent

Flight: E.g.,
personal information like
birthday, pass no., diets

Request for
Travel Plan



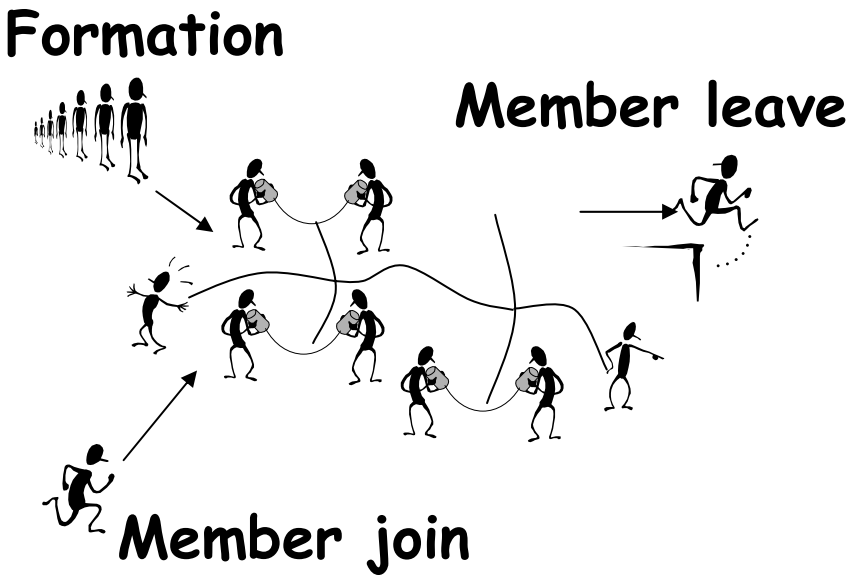
Intermediary

Hotel: E.g.,
physical handicaps

Car rental: E.g.,
driver‘s license

Law Enforcement

Changing Groups



What do we need?

Main Goal

- Multilateral Secure Computing Platform
  - Making own system ready for processing sensitive and legally binding data (protection of the user)
    - Isolation between all applications, trustworthy and non-trustworthy
  - Enforcing own security policies on foreign systems (protection against the user)
    - Labeling of all processed data
    - Labeled data is only processed on trusted machines

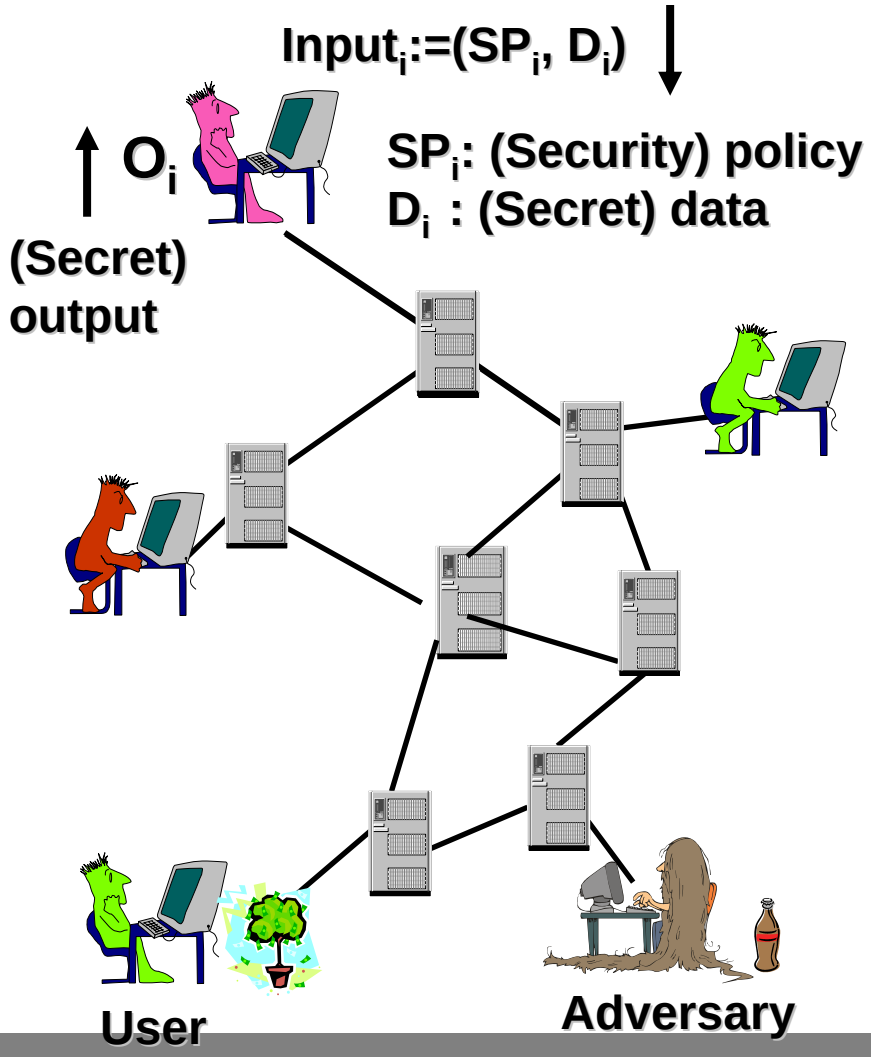
Secure Distributed Applications

Distributed Applications: Characteristics

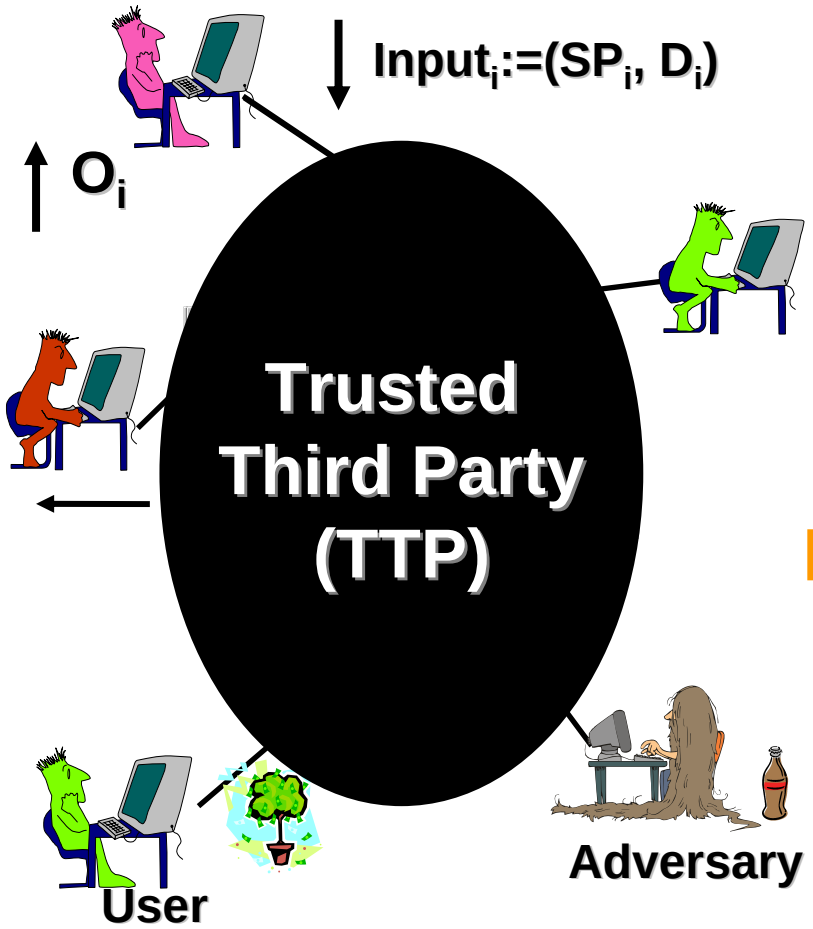
- Different principals involved
- Offer (require) services (resources)
- Different (conflicting) interests (policies)
- Distrust each other in general

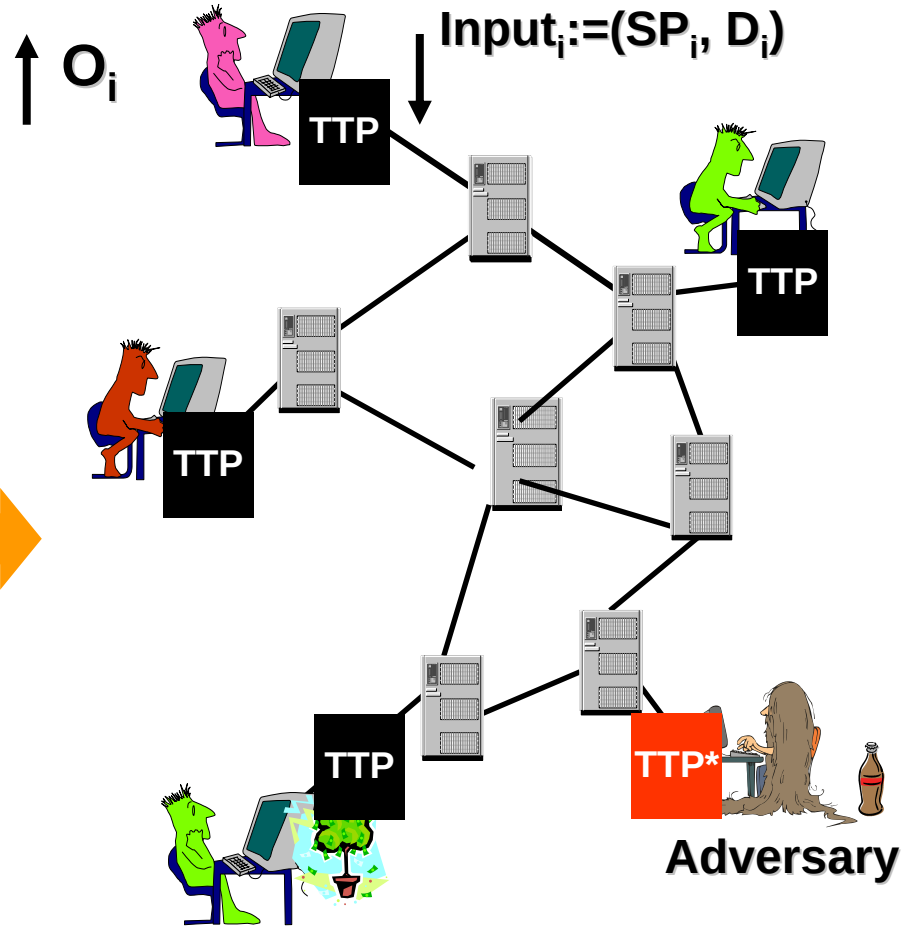
→ Multilateral Security

→ Classical security targets
  - Confidentiality
  - Integrity
  - Availability



Ideal vs. Real World

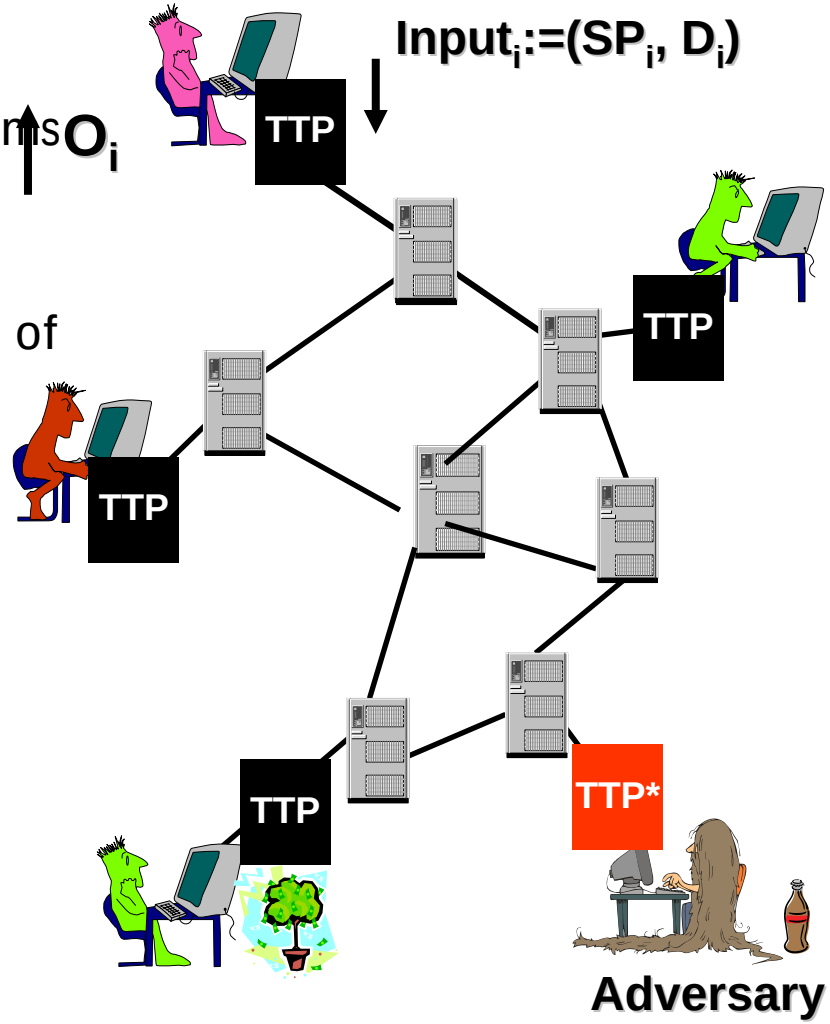




- Ideal world: TTP
  - Behaves correctly
  - Can access resources as required
- Real world: Each TTP
  - Should behave correctly but limited functionality and resources

Real World

- Goal
  - Trustworthiness: Computing platforms providing Multilateral Security
- Method
  - Attestation: Verify trust-worthiness of a remote platform/application



Application Scenarios

- E-Services
  - E-Government, E-Health, E-Commerce
- Enterprise Rights Management
- Digital Rights Management Systems
  - Copyright protection
- Supply chains
- Automotive
- Grid computing and outsourcing
- Next generation mobile devices
- Auctions
- First sale
  - making private copies
  - transfer of digital content

What is the Role of Trusted Computing?

Trusted Computing

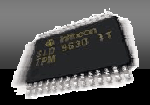
- Stated goal
  - Allows increased security for applications to be built without significant changes to computing platforms in use
  - Assured operation for applications on local and remote platforms
    - a limited set of functionalities is assumed to be correct (TCB)
      - Reporting state to remote party
      - Enforcing security policy locally against software attacks

- Based on “root of trust” concept
  - Implemented in hardware-based component since protection of sensitive data in software is difficult

- Some main Trusted Computing functionalities
  - Attestation (reporting state of a remote platform)
  - Strong isolation
    - Curtained memory (memory separation of processes)
  - Sealed storage (access control to data based on executing software stack)
  - Secure IO (assured input/output to peripheral)

Possible Formula: Trustworthy Platforms

Trusted Computing (HW)



Hardware

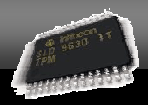
TPM, LaGrande, SEM, TrustZone

+

Trusted Software Layer

Trusted OS

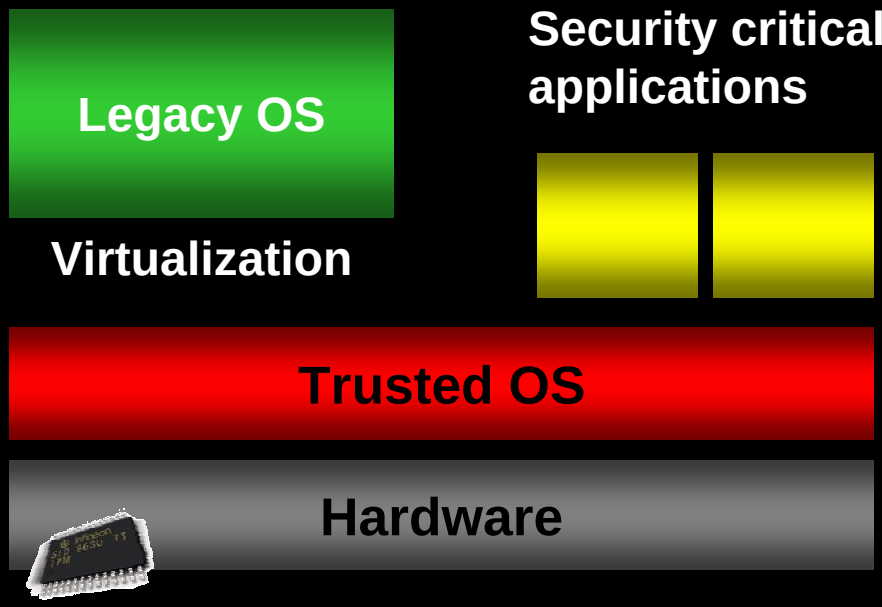
Hardware



TPM, LaGrande, SEM, TrustZone

+

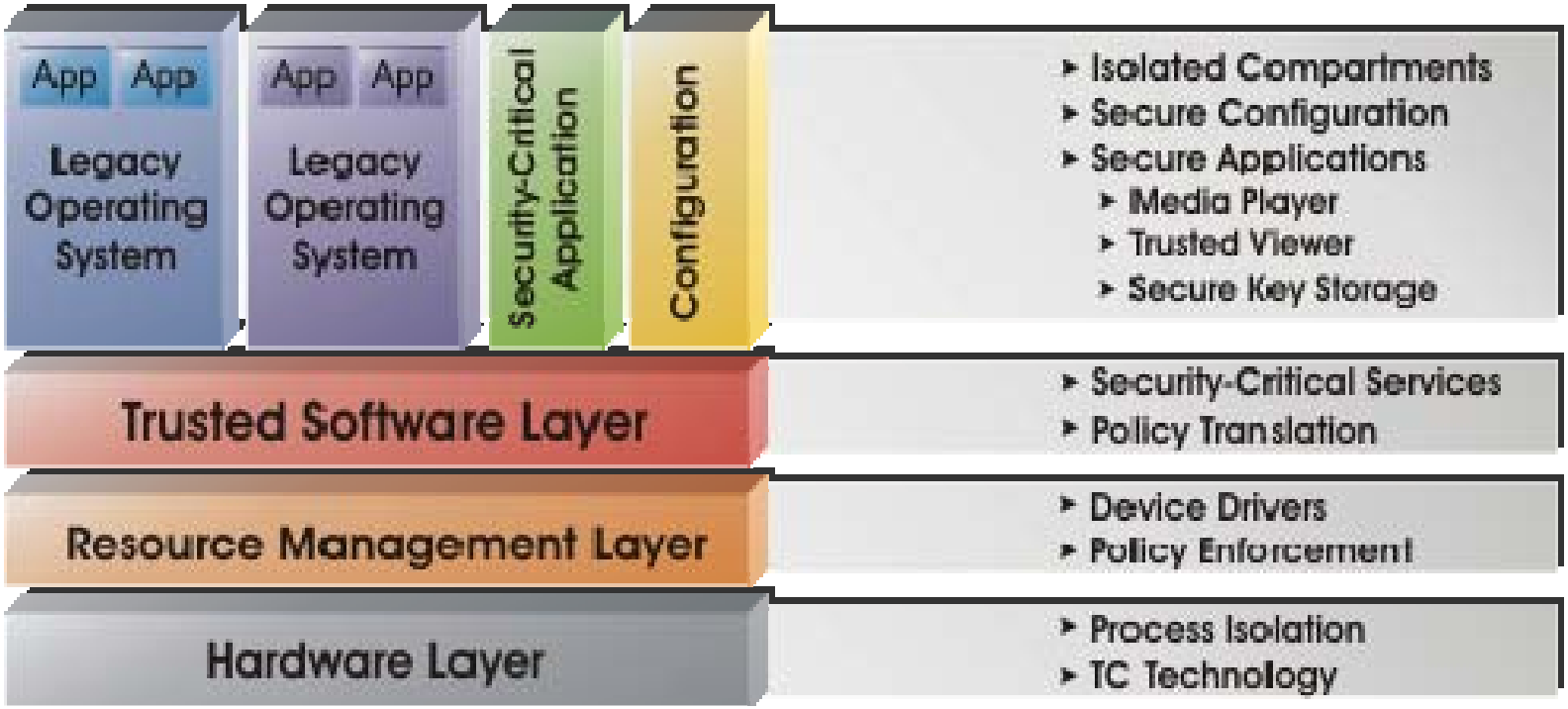
Legacy OS



TPM, LaGrande, SEM, TrustZone

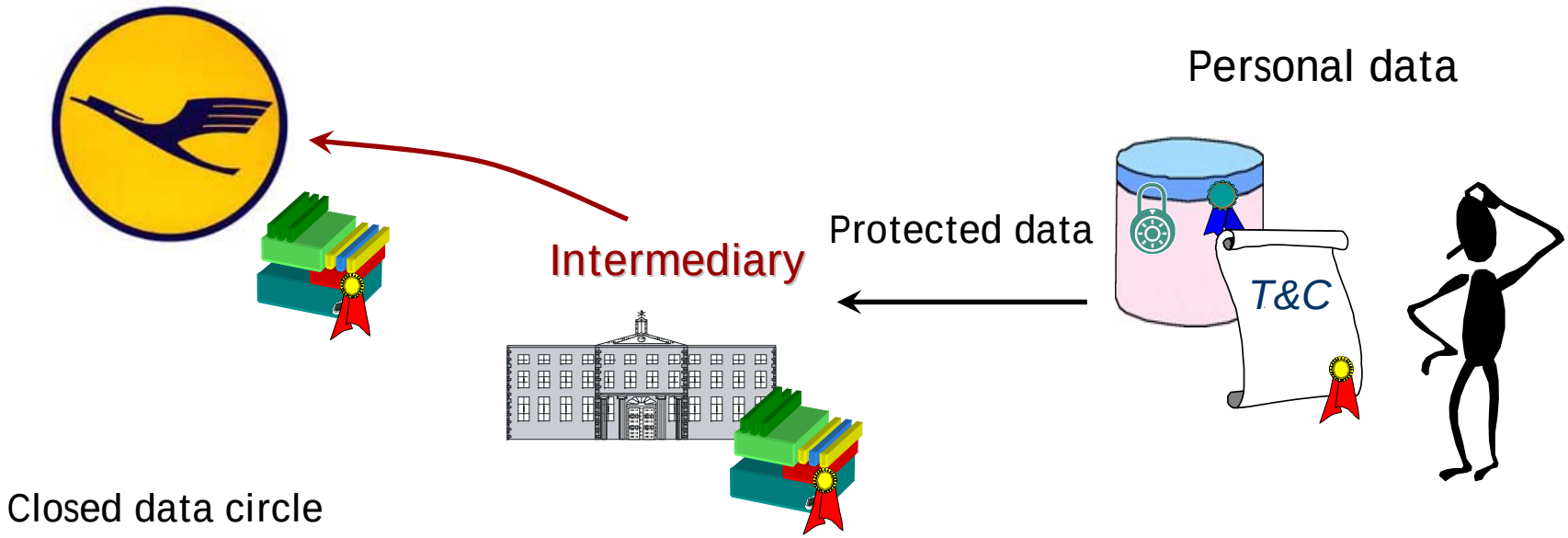
Security Architecture

- Our main research & development platform



Back to our Scenario…

Application Scenario



Trusted Computing Projects in Europe

Open Trusted Computing Project!

opentc.net

EMSCB-Project

emscb.de

European Multilaterally Secure Computing Base

www.emscb.org

EMSCB - Overview

- European Multilaterally-Secure Computing Platform
- Partly funded by German Ministry for Trade and Technology (BMWi)
- Developing an
  - open
  - multilaterally-secure computing platform
  - that is *secure enough* to allow new and innovative business models
  - Based on
    - PERSEUS/Nizza Security Framework

- Trusted Computing Conference in Berlin
  - 19. and 20. of October 2006
  - In cooperation with German Ministry for Trade and Technology (BMWi)

Bundesministerium
für Wirtschaft
und Technologie

Project Consortium

THE END ...

More Information available at

- http://www.sirrix.com
- http://www.fidis.net
- http://www.emscb.org
- http://www.opentc.net