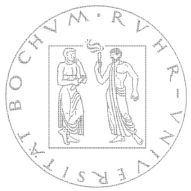
Turaya –
An Open Trusted Computing Platform



Ruhr-Universität Bochum

Prof. Dr. Norbert Pohlmann

Institute for Internet Security
University of Applied Sciences Gelsenkirchen
www.internet-sicherheit.de

European Multilaterally Secure Computing Base
www.emscb.org

Agenda

- Motivation / approach
- The EMSCB Project
- Trusted Computing Group
- Turaya security platform
- Summary

Turaya
→ Motivation

What we need is trustworthy IT that is achievable by means of a security platform

- which solves the **security problems** of existing computer systems or greatly restricts the harmful effects of e.g. viruses, worms, trojans, phishing, exploits, SW updates
- which guarantees the trustworthy processing of information on one's **own** and on **external** computer systems
- which supports the use of existing operating systems
- which offers transparent security or transparent trustworthiness

Turaya
→ Approach

What we need is **increased trustworthiness** through the **conception** and **development** of a **trustworthy, fair** and **open security platform.**

Trustworthiness

- Comprehensible architecture, low level of complexity of the technology
- Transparent implementation and **trustworthy execution**
- Functions that guarantee trustworthiness: sealing, attestation, secure boot

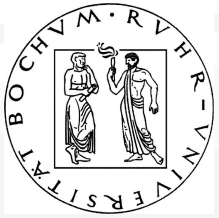
Fairness

- The enforcement of rights requires the **agreement of all parties**.
- The security platform **can be used, but does not have to be**.
- User (Data protection), Organisations (secure handling of important data), External bodies (copyrights and licences)

Openness

- Creation of an open standard to improve interoperability.
- Turaya can be used by all operating systems and platforms. (Desktop, SmartPhone, PDAs, embedded systems)
- Open to all partners - no discrimination against individual suppliers/users

The EMSCB-Project
→ Consortium Overview



Consortium manager

Ruhr-University-Bochum
eurobits

TECHNISCHE UNIVERSITÄT DRESDEN
Institute for System architecture

Fachhochschule Gelsenkirchen
Institute for Internet Security

Financed by the
Bundesministerium für Wirtschaft und Technologie

Sirrix AG security technologies

escrypt Embedded Security

Strategic industrial partners:

SAP

BLAUPUNKT Bosch Gruppe

Infineon

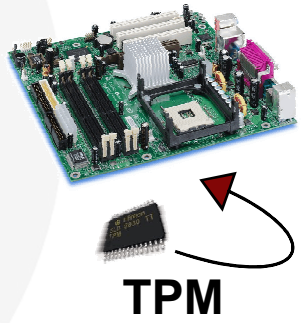
Trusted Computing Group
→ Organisation and Idea

- ***Trusted Computing Group (TCG):***
  Industrial consortium consisting of more than 160 leading IT companies (such as Hewlett-Packard, IBM, Intel, AMD, Microsoft, Sun, …, Infineon, Utimaco, G&D, ...)

- ***Fundamental motivation***
  - Develop **open specifications** for trustworthy IT systems (servers, PCs, embedded systems, etc.)
  - Improve the security of distributed applications at a **reasonable economic cost**
  - Avoid any extensive changes to existing hardware or software.
- ***Main Idea***
  - Manipulation-proof hardware component (securer than software)
    → **”improvement" against software-based attacks.**
  - Security of the system is reduced to the security of a security module.
  - The integrity and authenticity of an IT system can be reliably tested, even from a distance

Trusted Computing Group
→ Functions (1/2)

- ***Trusted Platform Modules (TPM)***
  - Reliable random generator (secure cryptographic keys)
  - Cryptographic functions: signature (RSA), hash function (SHA-1)
  - Creation of different cryptographic keys
  - **Platform Configuration Register (PCR) for storing the system configuration**.
- ***Secure Store***
  - Creation of secure cryptographic keys
  - Storage of these keys in the hardware module
- ***Sealing***
  - Cryptographic keys can be binded to the IT system and/or a specific software configuration.
    → Provide protection against manipulations of the operating system



Trusted Computing Group
→ Functions (2/2)

- ***(Remote) Attestation***
  - Analyse the current configuration of the IT system
  - Detecting manipulated IT systems (distributed systems, Web Services, …)
  - Communication only with trustworthy IT systems
- ***Access Control***
  - Implementation of access rules in a network with unknown IT systems (TNC)
- ***Trusted Boot***
  - System configuration can be checked (smartcard, USB stick, mobile phone)
- ***Installed TPMs***
  - 60 million by the end of 2006
  - 130 million by the end of 2007
  - 200 million by the end of 2008

TPM

Trusted Computing Group
→ Limitations and Reservations

- ***Limitations***
  - No solution for typical development errors
  - No trustworthy path to applications
  - No isolation of the applications from one another.

- ***Reservations***
  - **Restricted** interoperability → **Discrimination**
    → Binding of data to SW configurations
  - **Data protection** infringements
    → Exact information via an IT system is controlled
  - **Questionable** trustworthiness
    → Closed Source, no re-engineering

→ **Trusted Computing does not solve any security problems of existing operating systems, but can nevertheless check them**

→ Solution to these limitations: ***An appropriate security platform***

Turaya Security Platform
→ Basic Idea

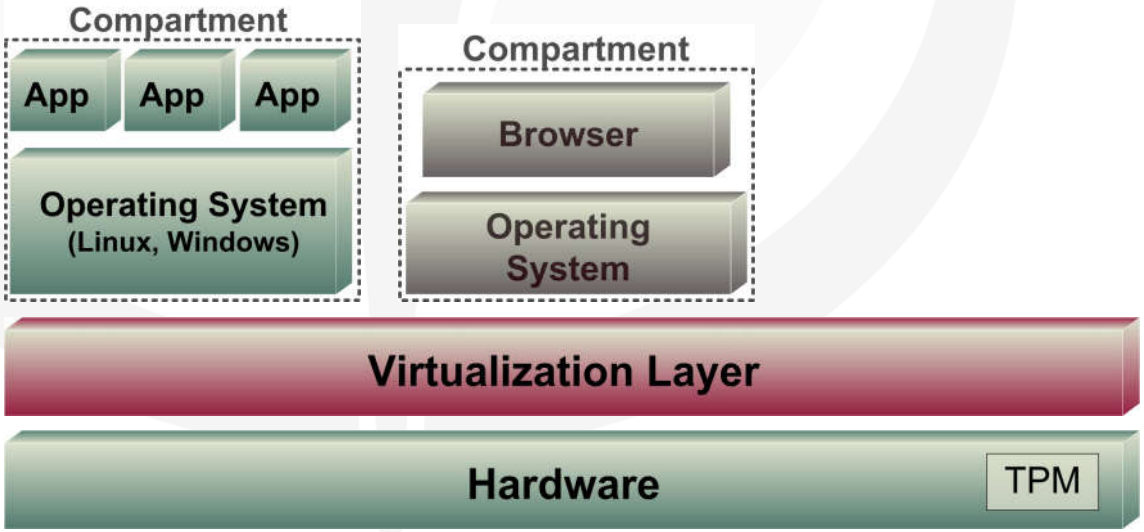
- Trusted Computing needs a security platform!
- The security platform requires special attributes such as:
  - **Trustworthiness**
  - **Fairness**
  - **Openness**
- With the Turaya security platform we enable Trusted Computing to be "open" within the meaning of our attributes.

Turaya Security Platform
→ Architecture and Technology 1/3

- ***Conventional hardware***
  - CPU / Hardware Devices
- ***TPM***
  - Highest level of protection through hardware-based security
- ***Use the advantages of Trusted Computing technology***

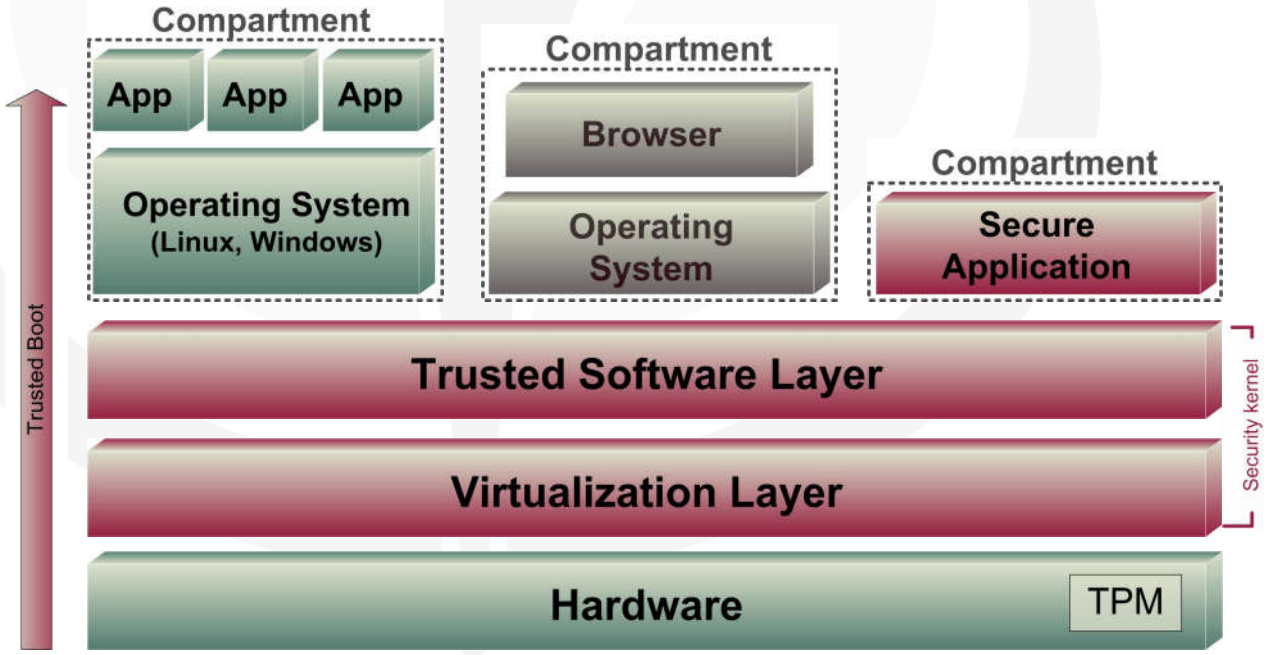
Turaya Security Platform
→ Architecture and Technology 2/3

- ***Virtualisation layer for the purposes of isolation...***
  - Protect applications
  - Protect user data
  - Protect against the manipulation of an application (e.g. browser)
- ***... through modern virtualisation technologies***
  - Micro-Kernel architecture
  - Use of existing components in compartments



Turaya Security Platform
→ Architecture and Technology 3/3

- ***Security Platform (Trusted Software Layer)***
  - **Authentication** of individual compartments
  - **Binding of data** to individual compartments
  - **Trusted Path**
    - Between user & application / application & smartcard
  - **Secure policy enforcement**



Turaya Security Platform
→ Additional Properties

- ***Minimalisation***
  - Error avoidance through the **modularity** and **low level of complexity**
- ***Openness:***
  - Design, sourcecode, documentation, standards
- ***A simple application***
  - Standardised management interface for all compartments
  - Small support requirement
  - High level of stability
- ***Compatibility & Interoperability***
  - Different operating systems and versions are possible in parallel
  - The security services are independent of the respective operating system

Turaya Security Platform
→ Application Scenarios and Lines of Business

- ***Financial Field***
  - Secure online banking
  - Secure communication
- ***Public Authorities and Companies***
  - Secure processes / communication / applications
  - eGovernment, ePassport, eVoting, health card
  - Qualified signature, secure middleware
  - Enterprise rights management (content / document protection)
- ***Content Providers / Commercial Sale***
  - eCommerce
  - Digital Rights Management (DRM)
- ***Secure Client Server Models***
  - External employees, secure supply chain, company communication
- ***Security in Embedded Systems***
  - Mobile devices, automotive

Turaya Security Platform
→ Milestones / Applications

- ***Turaya.Crypt***
  → Completed
- ***Turaya.VPN***
  → Completed
- ***Turaya.FairDRM***
  → Test phase
  A simple fair DRM system
- ***Turaya.ERM***
  → End of 2007 - **partner SAP**
  Policy-based document management
- ***Turaya.Embsys***
  → End of 2007 - **partner Bosch/Blaupunkt**
  Multimedial use of the platform in embedded systems

Turaya Security Platform
→ Pilot: Turaya.ERM (1/2)

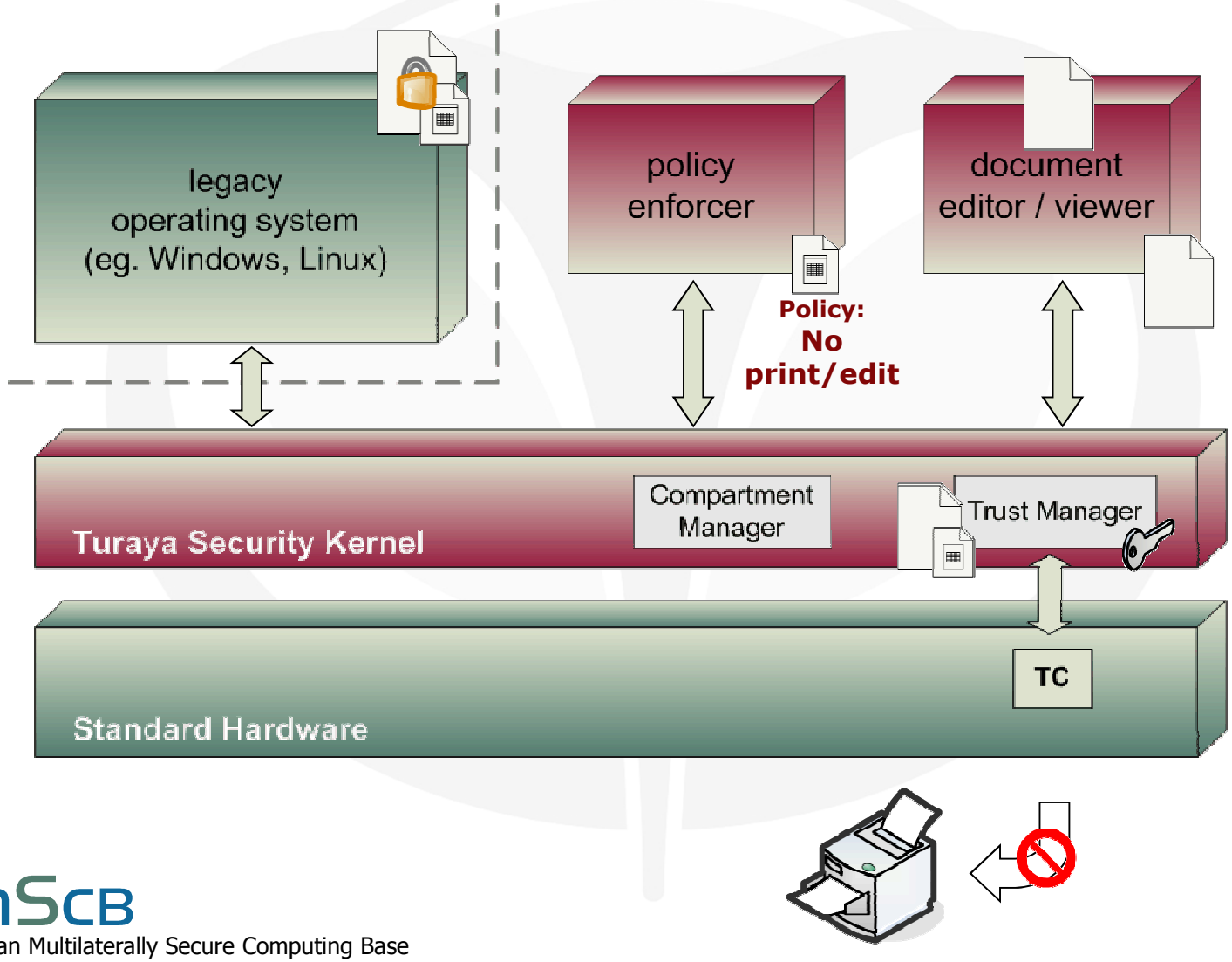
Fair Enterprise Rights Management (ERM)

- **Open** Security Platform which gives **equal** consideration to the requirements of the **content provider** and the **content consumer**
- Runs **parallel** to the conventional operating system
- Independently of conventional operating systems

Properties and services

- Licence negotiations
- Licence transfer
- Protection of user data

Turaya Security Platform
→ Pilot: Turaya.ERM (2/2)



Turaya Security Platform
→ Summary

Turaya:

- The Turaya security platform enables the trustworthy, fair and open use of Trusted Computing technology
- The Turaya security platform is freely available
- Turaya is one of the leading developments in the field of TC
- Important industrial partners develop interesting pilot applications together with the EMSCB Team.

→ Trusted Computing will spread anyway, but without Turaya to an extent over which the user has little influence!

→ Come and join us:

- Profit from the direct dialogue with cutting-edge IT security research
- Influence the next developments
- Take advantage of this opportunity for your company

Come and join us

The EMSCB-Project

www.emscb.org

Prof. Dr. Norbert Pohlmann

Institute for Internet Security
University of Applied Sciences Gelsenkirchen
www.internet-sicherheit.de

European Multilaterally Secure Computing Base
www.emscb.org