The Role of Trusted Computing for Identity Management

Dirk Kuhlmann,
Trusted Systems Lab
HP Laboratories Bristol
dirk.kuhlmann@hp.com

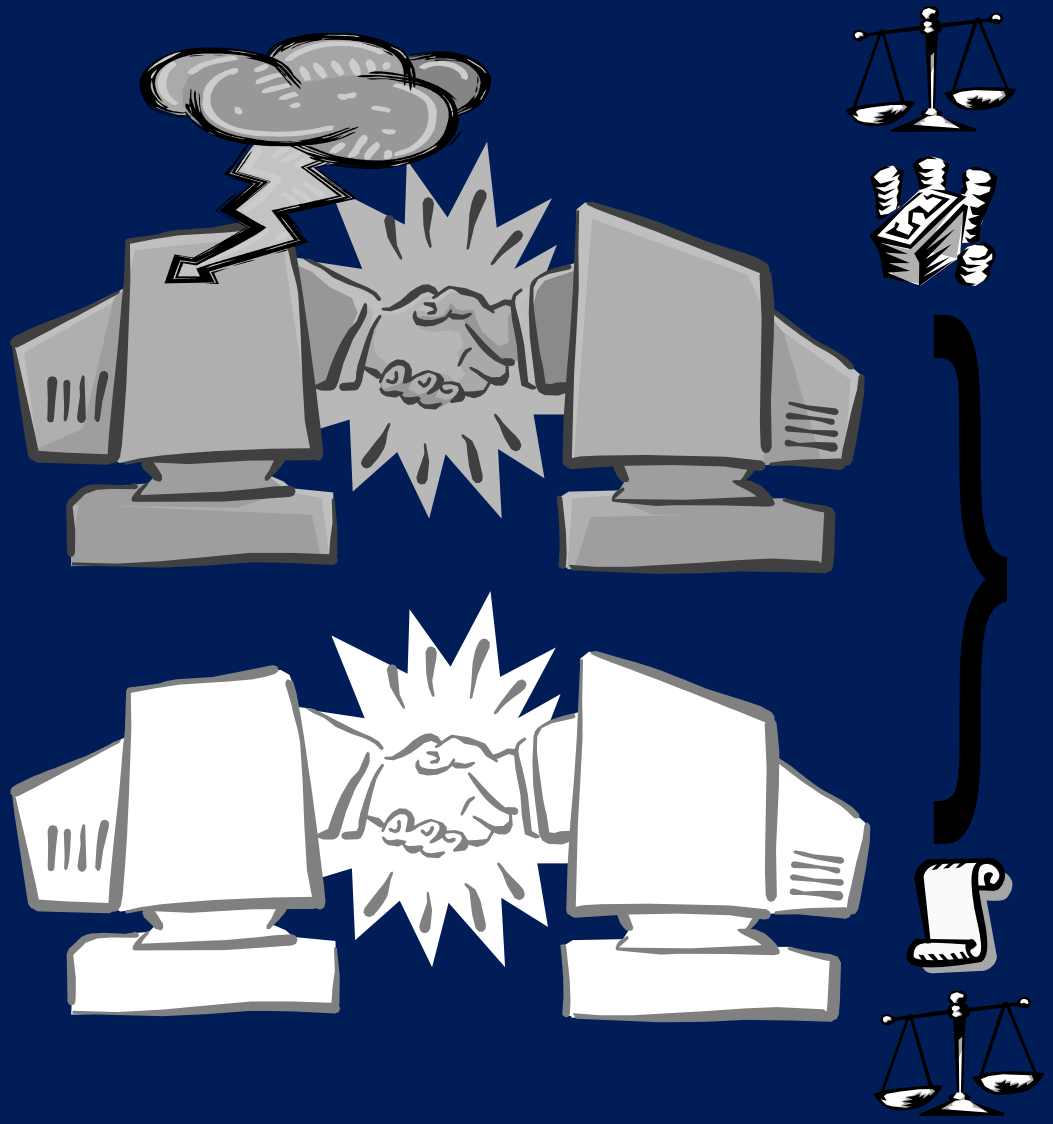
‘Identity’ – Misnonmer or Very Useful Concept?

- In mathematics, ‘==‘ is a reflective, symmetric, transitive relation
  (a == a) ; (a == b) => (b == a) ; (a == b) ^ (b == c) => (a == c)
- In philosophy, *personal identity* concerns the conditions under which a person at one time is the same person at another time.
- In the social sciences, *social identity* concerns the individual's comprehension of him or herself as a discrete, separate entity.
  - There’s more than one: cultural, gender, legal (id)entity, …
  - Often better to think roles and contexts here.
- Object Identity (OOP): property of objects that allows those objects to be distinguished from each other, identifiability.
- Digital Identity is the representation of identity in terms of digital information.
- Digital Identity Theft is the deliberate appropriation of someone else's digital identity (without that person's permission) for criminal purposes.

Trusted Computing – Identifiable Expectations

- Trusted Platforms (TPs) behave in an expected manner for a particular purpose and particular time.
  - Multiple purposes reflected in multiple roles aka platform dentities
  - Pseudonymous or quasi-anonymous identities are supported
  - Scalable non-linkability with (AIKs) or without (DAA) trusted third parties
- TPs can attest their fitness for purpose to remote peers
  - Bootup, configuration, system state
  - How can we build up expectations about remote behaviour?
- TPs provide HW supported protection of keys, data, logs, and execution environments.
  - Bind data to one or more platforms or owners
  - Tamper protected auditing subsystems
  - Security enhanced execution compartments (OS, applications) for critcal software
- If we have more confidence in the behaviour of a remote system, we might require less information about its user.
  - Hence – less knowledge about his 'true' social identity

TC, Identities and Communication Contracts



- Present
  - TCP/IP + user authentication are entrance ticket
  - User auth says little about exposure to risk
  - User authorization discloses aspects of social identity
- Future
  - Attest fitness for purpose
  - Scan for vulnerabilities before admission to the network
  - May help to minimize exposure of social identity
  - Allows for multiple roles

OpenTC: Project in a Nutshell

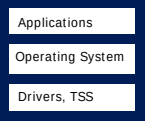
Chosen vehicle: Collaborative, academic/industrial research project funded by the EC

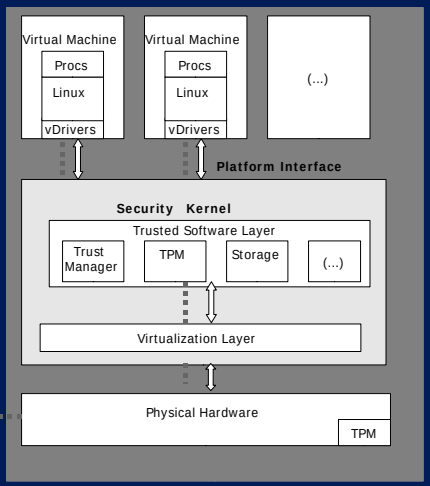
- 23 Partners
  - Academic: University Cambridge (XEN) , Univ. Dresden and Bochum (microkernel based security architecture)
  - Industrial: AMD, Infineon, HP, IBM, SuSE/Novell
- Integrated Project, Duration: 36/42 months, Active since December 2005

- Work Packages: Hardware, Virtualization Layers, Distributed Management, Validation/QA, Mobile Platforms

- Address most critical issue: fear of customer lock-in
  - Explore TC for Open Source based system
  - Architecture to support maximum flexibility and choice
  - Introduce fnew perspectives into public debates
  - Include TCG members who also are OSS stakeholders

- Political/geographical context
  - Main debate happened in Europe





OpenTC: Architectural Goals

Virtualization Layer providing ‘Compartments’

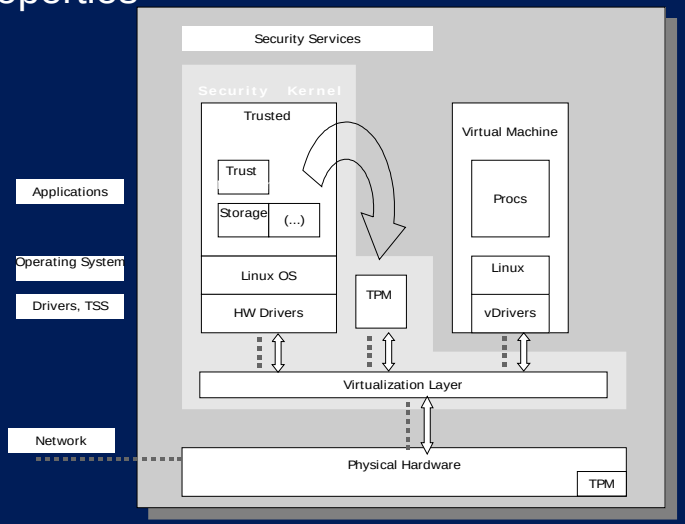
- Audited and attestable boot-up of VMM and platform management components
  - Uses TC trusted boot
- Virtual Machines with information flow policies enforced by the VMM / secure services
  - Configuration and Policy are attestable
  - ‘Customer Compartments’ with remotely attestable properties

Explore next generation x86 CPU features

- Improved protection mechanism for memory and I/O
- Secure initialization
- HW Support for virtualization

Explore features of v1.2 Trusted Platform Modules

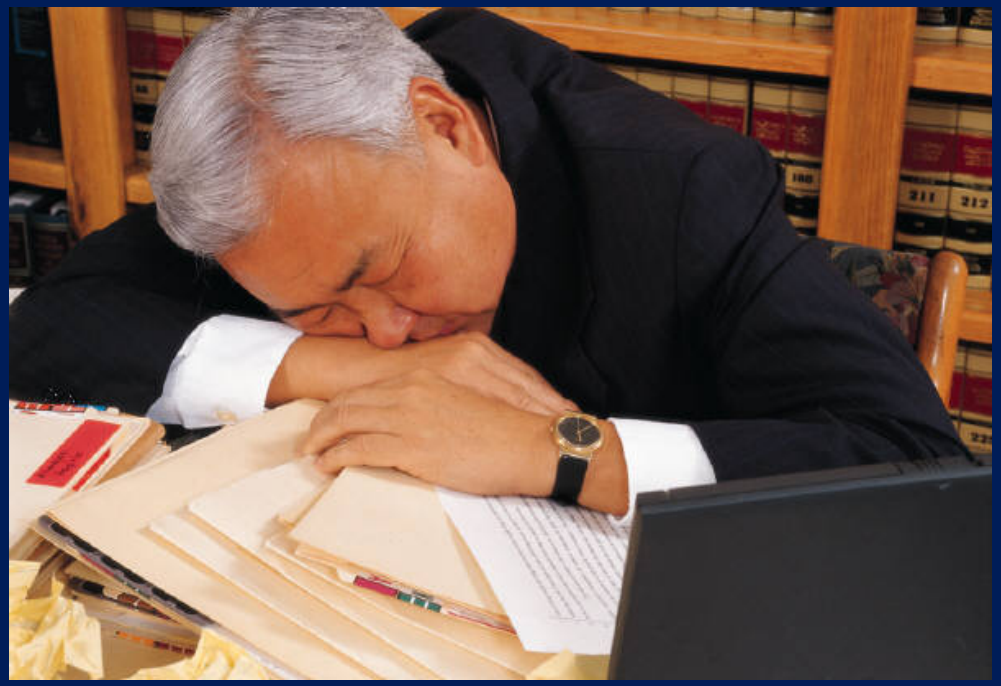
- Support for I/O (locality)



- **Looking for partners to adopt and explore this architecture in FP7 projects and supportive actions.**
- **In particular for testing, reverse documentation, reverse**
- **specification, validation of design and implementation.**

OpenTC

- Thank you for your time and attention!
- Questions?



- Contact:
- dirk.kuhlmann@hp.com

- Team:
- Chris I. Dalton
- David Plaquin
- Melvin Anderson