ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Trusted Knoppix

Master Thesis WS 2005/06

Thomas Zweifel, zweifelt@student.ethz.ch

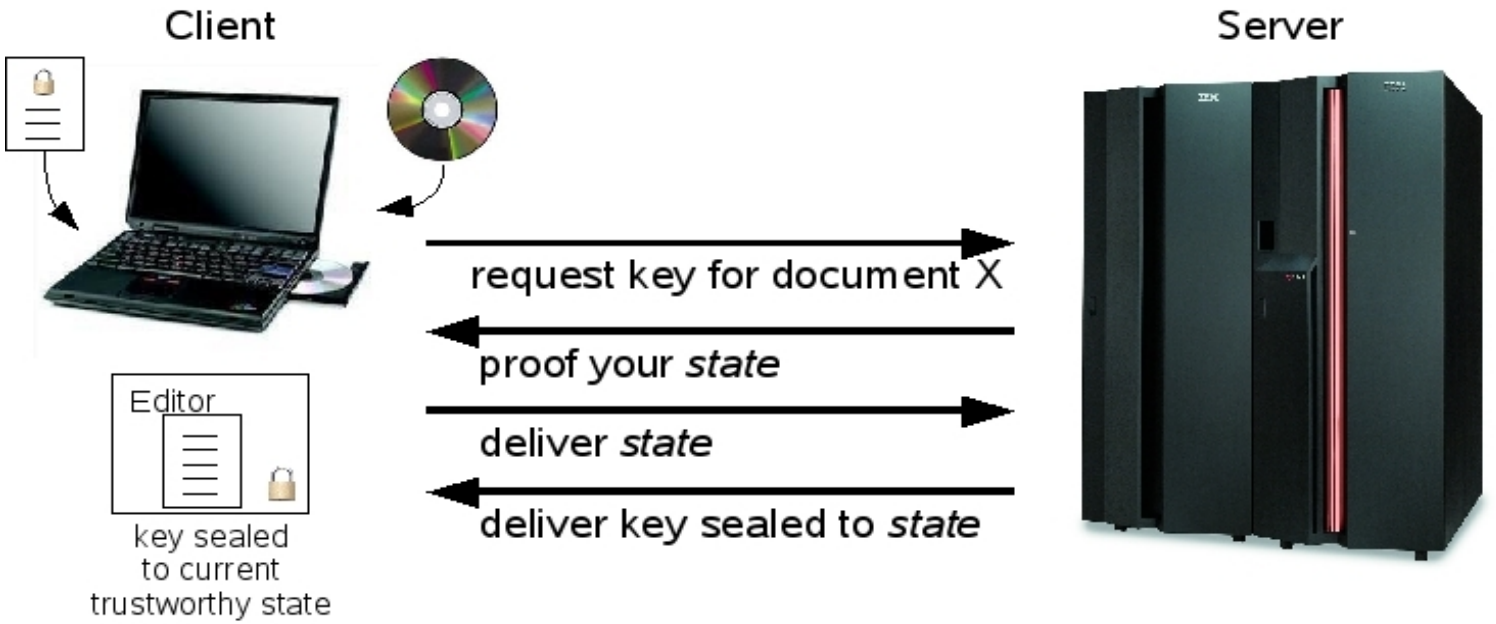
Prof. Dr. David Basin
Paul Sevinç
Mario Strasser

Overview

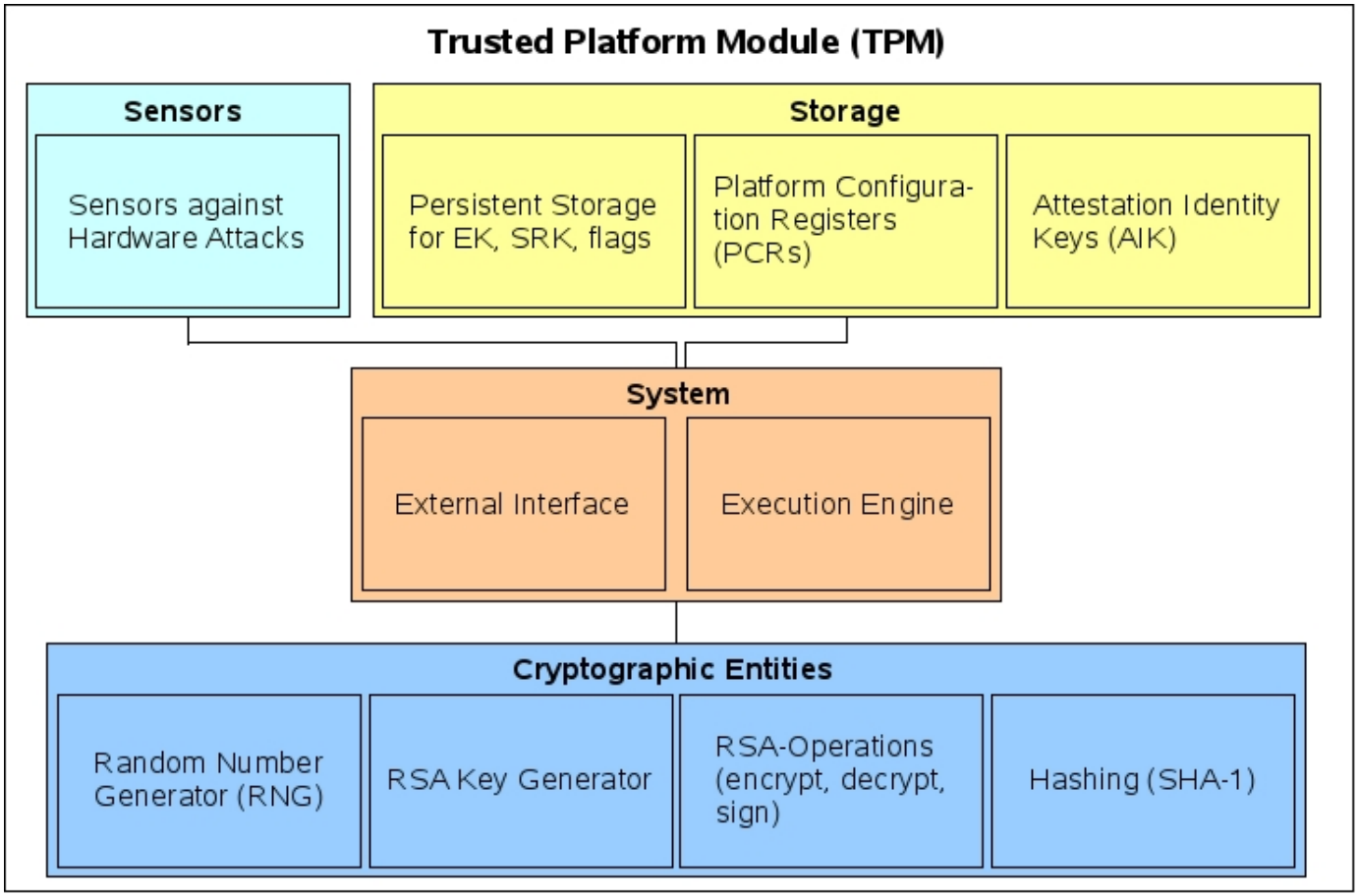
- Introduction
- Trusted Computing
- Protocol for Exchange of a Secret
- Conclusion

Introduction

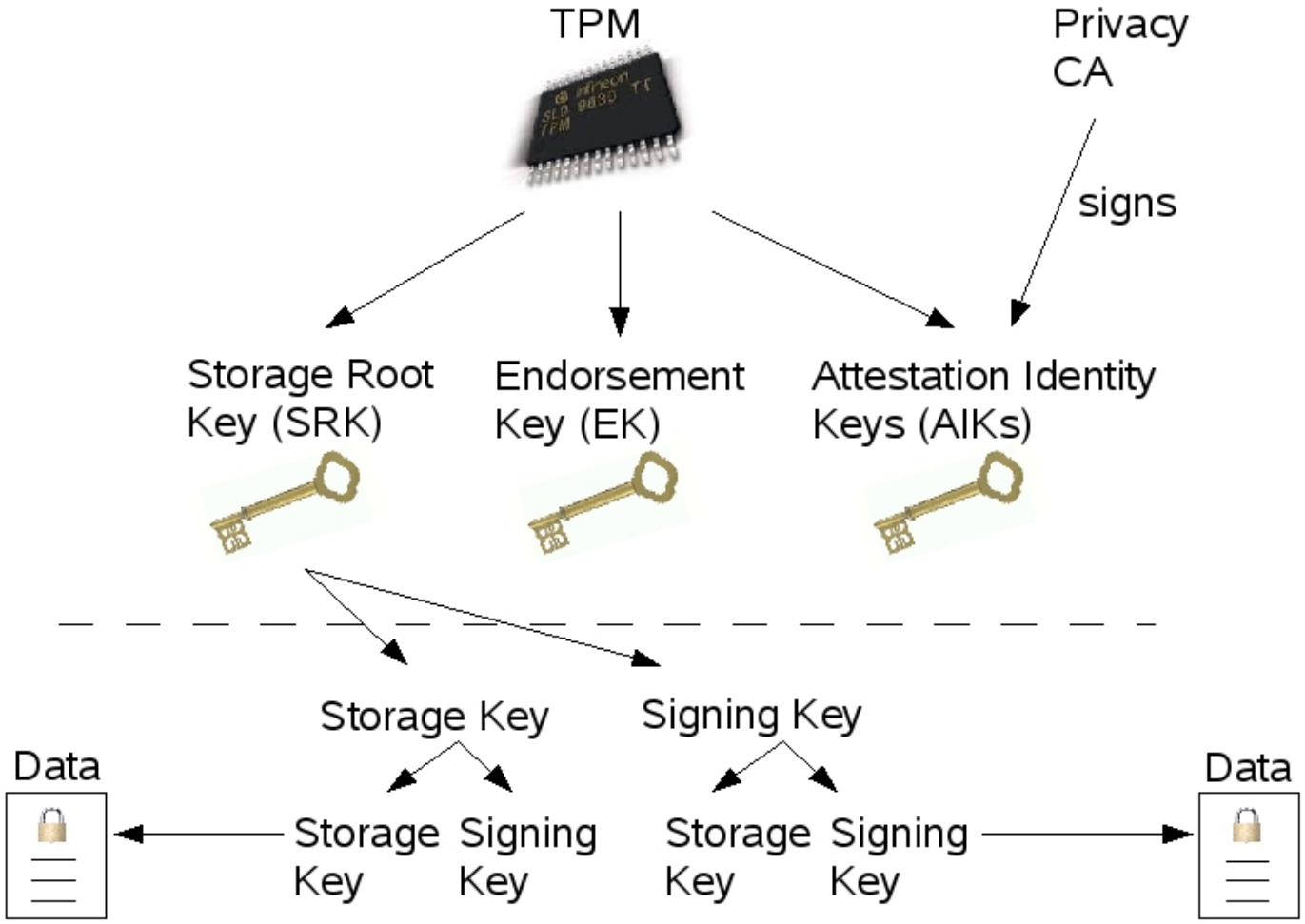
Introduction



Trusted Platform Module



Key Hierarchy

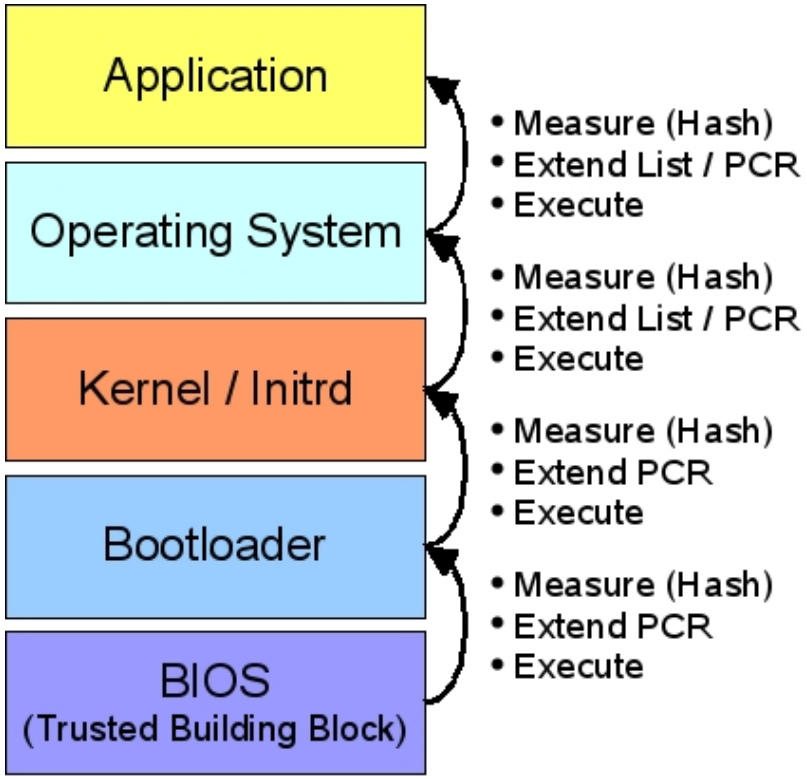


TPM Features

- Integrity measurements
  - Identify software by hash values
- Secure attestation
  - Fraud resistant attestation of the measurements
- Sealing and Binding
  - Allows to seal data to a defined state

Authenticated Boot

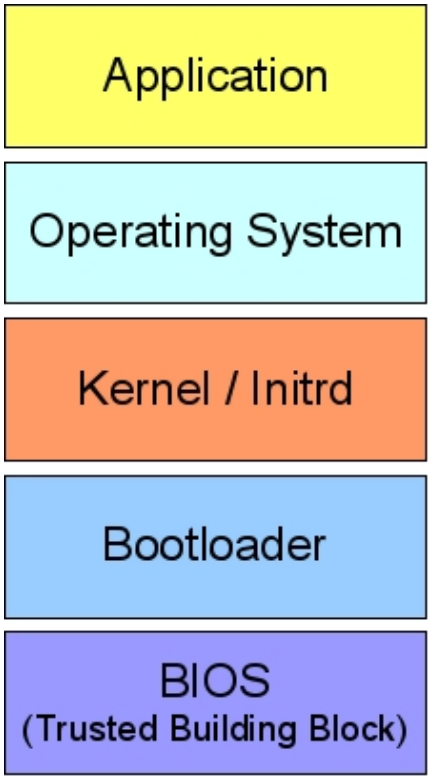
- Transitive Trust: Measure before execution



Actions

- Hash files
- Extend Register (PCR)
  $PCR_{t+1}=SHA1(PCR_t|hash)$
- Quote Registers
- Bind / Seal data to PCRs

Existing Projects for Linux

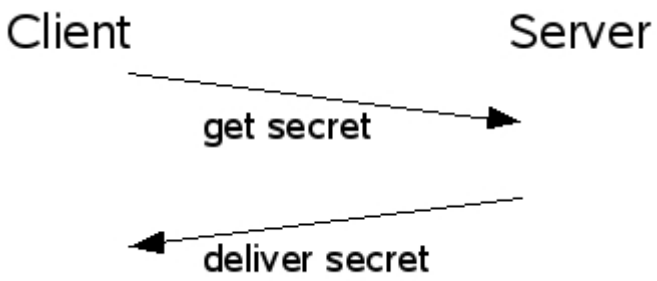


IMA: Integrity Measurement Architecture
Trousers: Trusted Software Stack

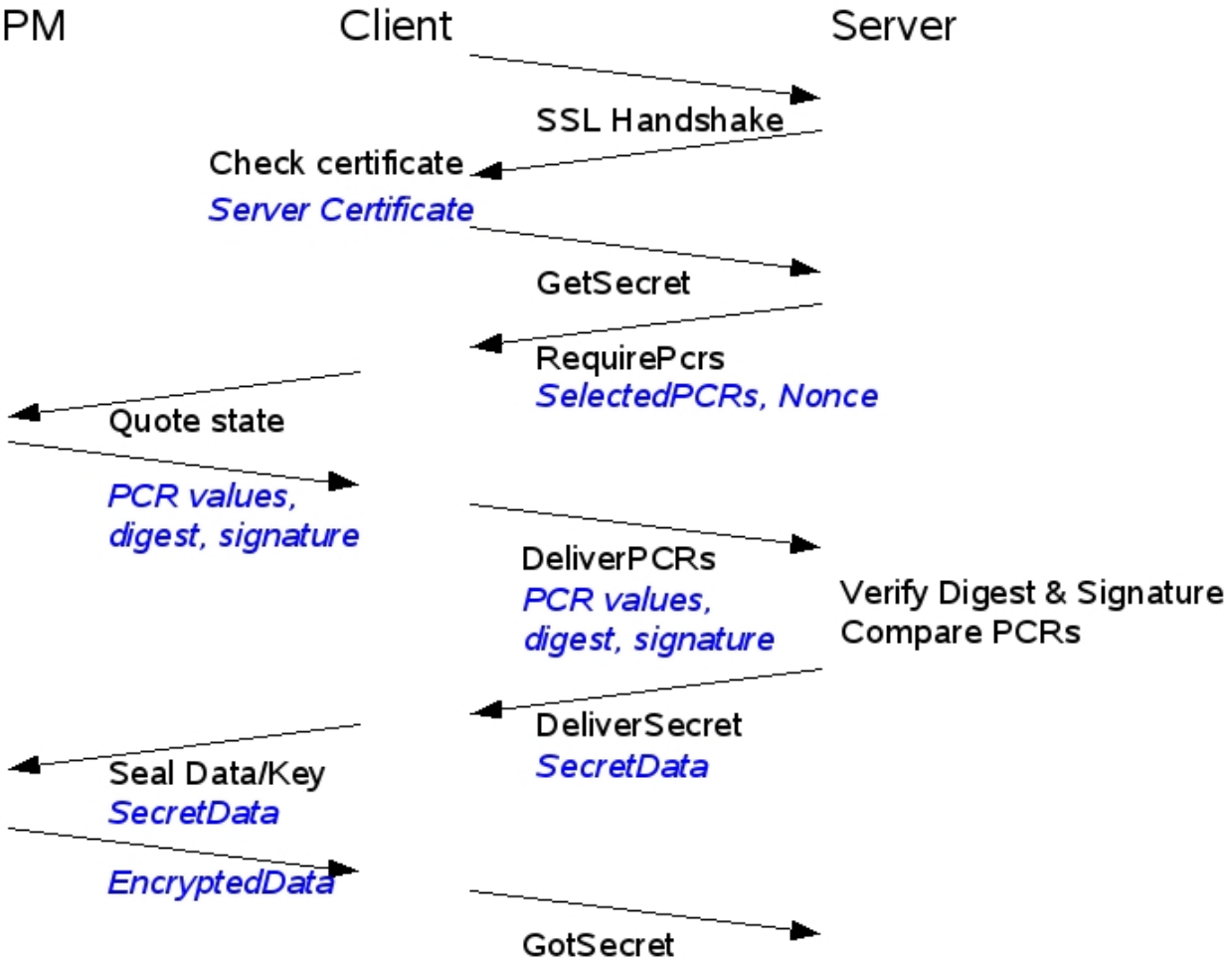
TPMdd: Device Drivers for TPMs

trustedGrub: TCG complying Bootloader

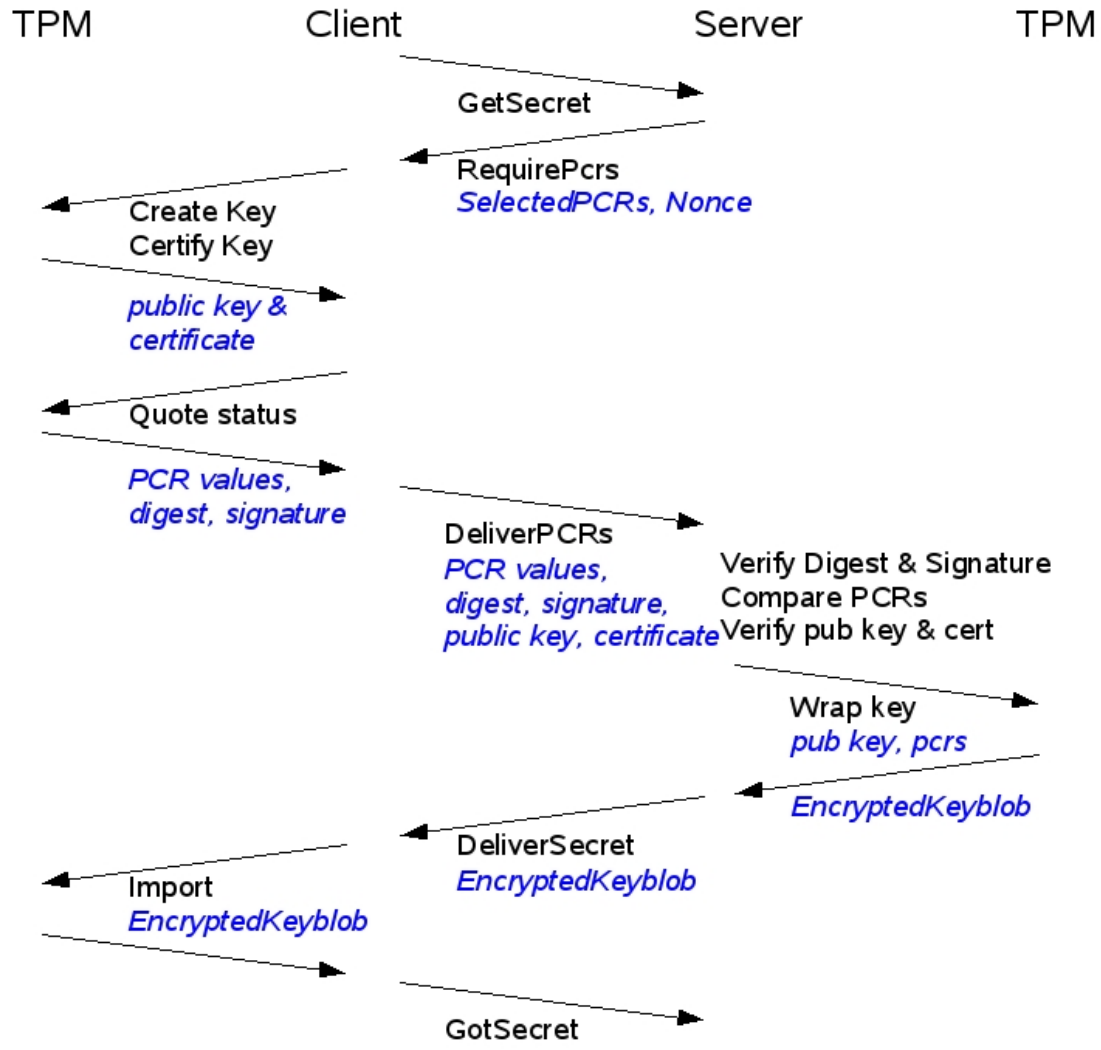
Initial Protocol



Protocol using SSL/TLS



Protocol without SSL



Conclusion

- Two Protocols developed
- Implementation uses SSL/TLS
- Migration to Knoppix
- Privacy concerns
  - Currently, the server can identify each TPM
  - Introduction of an additional layer
    - Privacy Certification Authority as Trusted Third Party
    - Direct Anonymous Attestation