Secure Data Management in Trusted Computing

Ulrich Kühn
Deutsche Telekom Laboratories, TU Berlin

Klaus Kursawe (KU Leuven)
Stefan Lucks (U Mannheim)
Ahmad-Reza Sadeghi (RU Bochum)
Christian Stüble (RU Bochum)

CHES 2005

Roadmap

Introduction

Problems with Sealed Data

Platform Updates

Hardware Migration

Conclusion

TCG's Proposal for Trusted Computing

Trusted Computing Group: Industry consortium to devolop specifications to

> *[...] protect and strengthen the computing platform against software-based attacks.*

Key Idea: **Base Trusted Computing Base on small piece of secure hardware.**

Recent developments: TNC

Our Motivation: TCG hardware widely deployed
$\longrightarrow$ Combine with secure operating systems to increase security
Here: **Address problems and propose solutions.**

Trusted Platform Module

Main components:

- Cryptographic engine
- Non-volatile tamper resistant storage
  - Storage Root Key SRK $\rightarrow$ virtual shielded storage
- Endorsement Key
- Platform Configuration Registers PCR
  - write access only via Extend operation

Needs support by Trusted Software inside TCB.

Main TCG Mechanisms

- **Integrity measurement**
  - Establish platform configuration at boot time
- **Attestation**
  - Attest platform configuration to remote party
  - (Subset of) PCRs signed with Attestation Identity Key
- **Sealing**
  - Exclusive availability of information for certain configurations
  - TPM-enforced
- **Maintenance** for hardware migration

Integrity & Boot Process

Establish Chain of Trust for TCB:

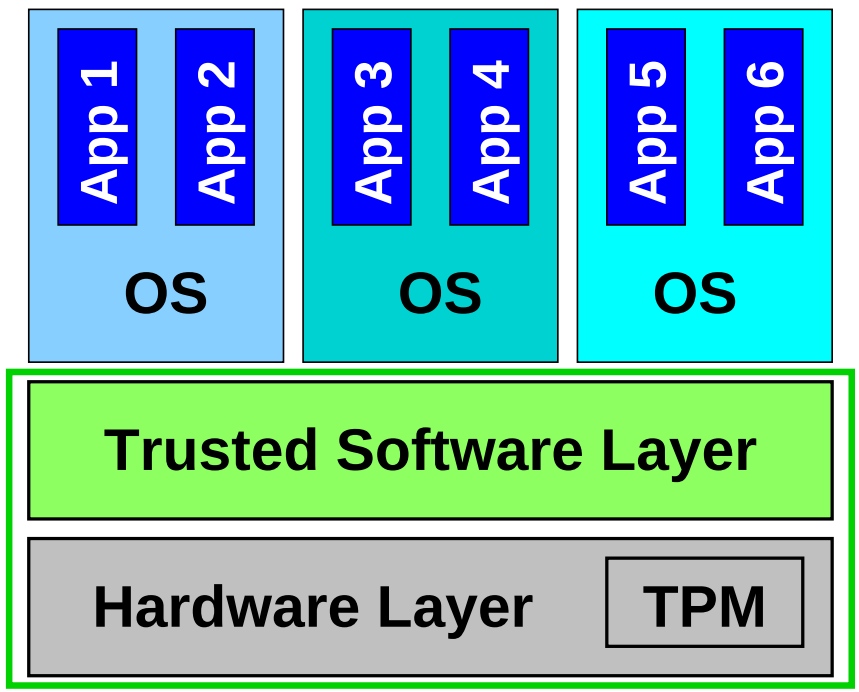
- Start from the Core Root of Trust
- Measure: $c \leftarrow \mathrm{SHA1}(\text{next software chunk})$
- Extend PCR: $PCR_i \leftarrow \mathrm{SHA1}(PCR_i, c)$
- Execute software chunk
  - might enter another measure-extend-execute cycle

Results:

- PCRs specific for current platform configuration
- Link between PCRs and software / security properties?
- Changed software not blocked but detected

Architecture of Trustworthy Platforms

Use TCB comprised of hardware and software:



- TPM
- Trusted software
- OS runs on top

Sealing

Places data in encrypted blob:

- Availability of data depends on predefined PCR values
- TPM delivers data only if those PCRs are present
- otherwise data remains encrypted

Usage Scenarios:

- Cryptographic keys for accessing networks
- Documents, Media files, etc.

Key question:
What happens to sealed data when patching the TCB?

Roadmap

Sealed Data & Platform Updates

Consequences of integrity measurement:

- Changing software in TCB changes hashes
- Results in changed PCR values
- Unseal does not release sealed data

- Intended for malicious / non-trustworthy "TCB"
- What about patches?
  - Typically preserve security properties
  - Should close security holes

Cannot distinguish good and bad changes!

Sealed Data & Hardware Migration

Maintenance procedure:

- Process is optional
- To our knowledge not implemented in existing TPMs
- Works only for TPMs of same vendor
- Needs interaction with vendor
  - Vendor out of business?
  - Price?

Availability of sealed data when HW breaks?

Roadmap

Introduction

Problems with Sealed Data

Platform Updates

- Software-Supported Updates
- TPM-Supported Updates
- Property-Based Sealing

Hardware Migration

Conclusion

Platform Updates

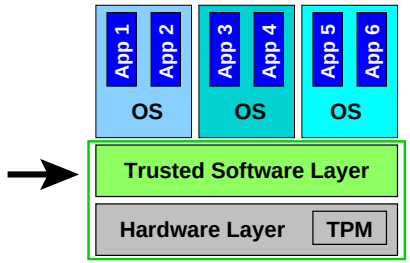
Requirements for a patched TCB:

- Security: Remote party wants that new platform configuration still adheres to security policy.
- Availability: Owner / User wants information available after patch.

Our solutions:

- Software-supported
- TPM-supported
- Property-based sealing

Software-Supported Updates



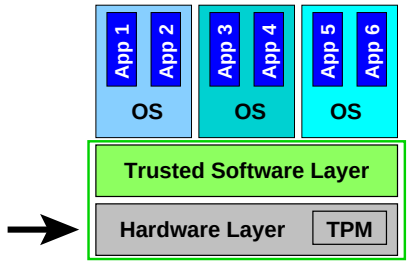
TCB component "Update Manager":

- Keep record of sealed data blobs
- Know new PCR values
- Ensure adherence to security policy
  - Signature by Trusted Third Party → Key management
- Be fail-safe

Pros & Cons:

- Works with current TCG hardware
- Handles only data sealed for current configuration
- Requirements for TCB design
- Difficult for parallel OS instances, e.g. bootloader updates

TPM-Supported Updates



Key ideas:

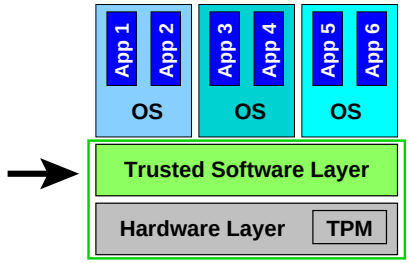
- New TPM command `TPM_UpdateSeal`:
  - Data sealed for S_i is resealed for S_j
- Delegate decision on equivalence of PCR values S_i and S_j
- Trusted Third Party issues update certificate

$$cert_{\text{update}} = \text{Sign}(S_i, S_j)$$

Pros & Cons:

- New TPM command, but should be easy to implement
- Avoids problems of software-only solution

Property-Based Sealing



Key Ideas:

- Seal data for abstract properties
  - e.g. "Strong Process Isolation"
- Mapping between properties and binary measurements

Pros & Cons:

- Better model for security functionality
- Resolves problems with handling sealed data
- Hides concrete binary measurements $\longrightarrow$ privacy
- To do: describe useful properties

Implementing Property-Based Sealing

Use TPM-support for property-based sealing:

- Describe properties by abstract configuration
- Data is sealed for abstract configurations only
- `TPM_UpdateSeal` translates to binary measurements
- Update certificate states that configuration implements security properties

Pros & Cons:

- Elegant solution for update problem
- Avoids discrimination of operating systems

Roadmap

Migrating to another Hardware Platform

Requirements for TPM migration:

- Completeness: Move secret state of source TPM to destination TPM; clear source afterwards.
- Security: Migration only if destination TPM at least as secure as source TPM.
  $\longrightarrow$ Delegate decision to trusted third party.
- Fairness: openly specified process
  - No need for interaction with vendor

Design of Migration Protocol

Key ideas:

- Secure export of non-volatile memory etc. under SRK
- Delegate decision on equivalent security of TPMs
  - Trusted TPM Migration Authority TMA
  - Migration certificate on TPM identities (endorsement keys) EK_s and EK_d

$$cert_{\mathrm{mig}} = \mathrm{Sign}(\mathrm{Hash}(EK_s), \mathrm{Hash}(EK_d))$$

- Special export mode for source TPM that allows only:
  - Extract SRK_s encrypted under EK_d
  - Clear TPM

Summary and Conclusion

- Update & migration problems with sealed data
- Proposed solutions for update issue
  - Software-only
  - TPM-supported
  - Property-based sealing
  - Combining TPM-supported with property-based solution
- Proposed secure & fair migration protocol
  - Improves over currently optional maintenance feature

- Ongoing work: TC-project at RU Bochum implements property-based sealing and attestation, see

www.emscb.org