Einführung in die TCPA Sicherheitskonzepte

Michel Messerschmidt

Gliederung

- Allgemeine Informationen
  - Wer, Was, Definitionen
- Systemintegration
  - Hardware
  - Software
- TPM - Funktionen und Dienste
  - Integrität
  - Geschützer Speicher
- Probleme
- Fazit, Ausblick

Was ist die TCPA ?

- TCPA = Trusted Computing Platform Alliance
- gegründet von HP, IBM, Intel und Microsoft
- 200+ Mitglieder (die Mitgliedsliste wurde lange Zeit geheim gehalten!)
- existiert seit Oktober 1999
- „An industry work group focused on enhancing trust and security on computer platforms“

TCPA war gestern...

- Gründung der TCG („Trusted Computing Group“) am 8.4.2003
- gegründet von AMD, HP, IBM, Intel und Microsoft
- im Vergleich zur TCPA stärkere Betonung „offener Standards“:
  - „To enable open standards development, the group is incorporated, has a patent policy and will provide industry advocacy programs, including a logo and marketing program“
  - Mehrere Mitgliedsstufen mit jährlichen Beiträgen von $7.500 bis $50.000

[Quelle: „http://www.trustedcomputinggroup.org/about/faq“]

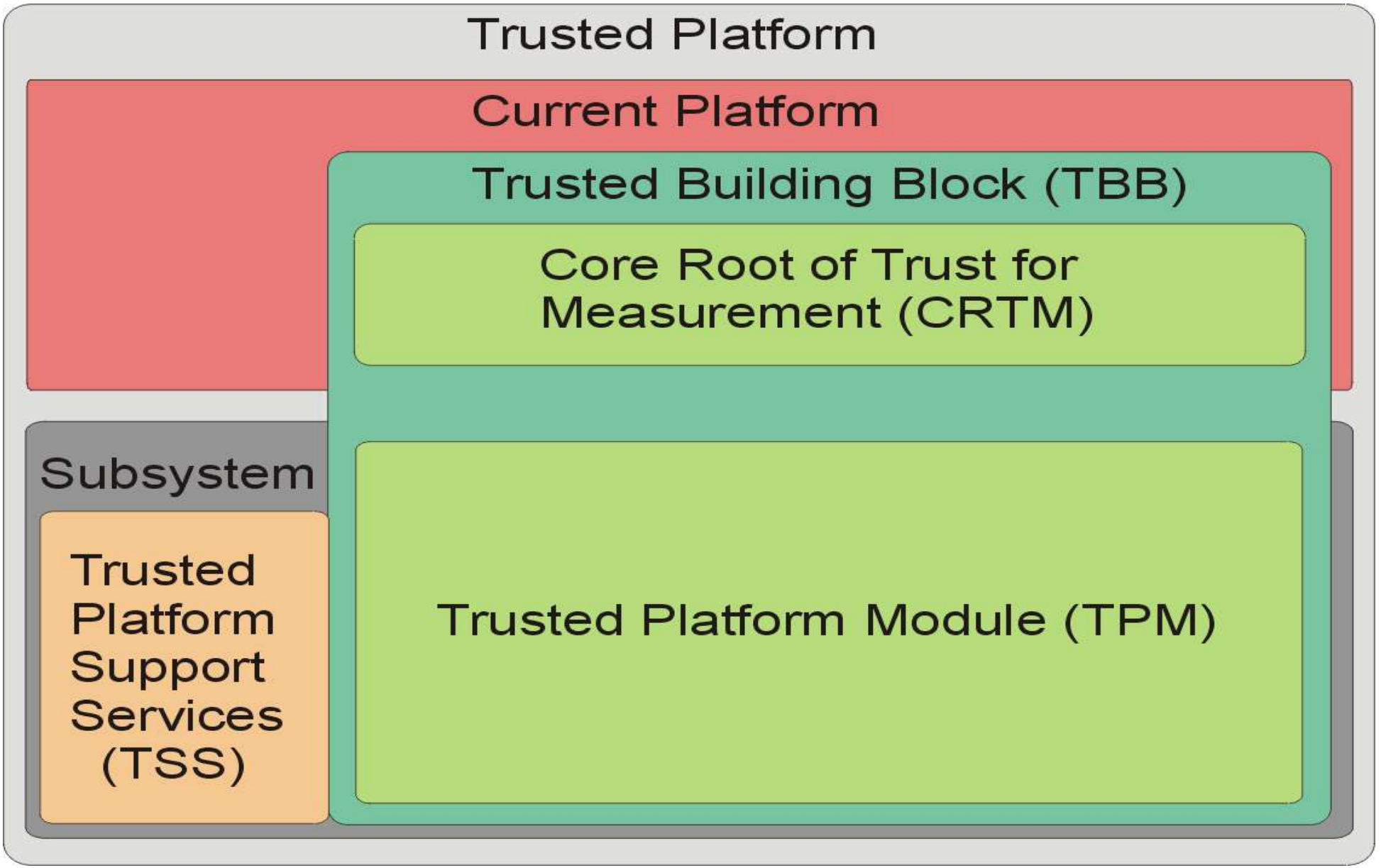
Ziele der TCPA / TCG

- Entwurf einer Spezifikation die Vertrauen in Computer schafft
  - zur Zeit öffentlich einsehbare Spezifikationen:
    - TCPA Main Specification v1.1b
    - TCPA PC Specific Implementation Specification v1.00
    - Trusted Platform Module Protection Profile v1.9.7
  - In Arbeit bzw. noch nicht veröffentlicht:
    - TCG TPM Specification v1.2 wird wohl noch 2003 veröffentlicht und soll bessere Übereinstimmung mit Palladium bzw. NGSCB (Next Generation Secure Computing Base) bieten
    - TCG Trusted Platform Support Services Specification v1.0
- Werbung und Unterstützung für die Umsetzung

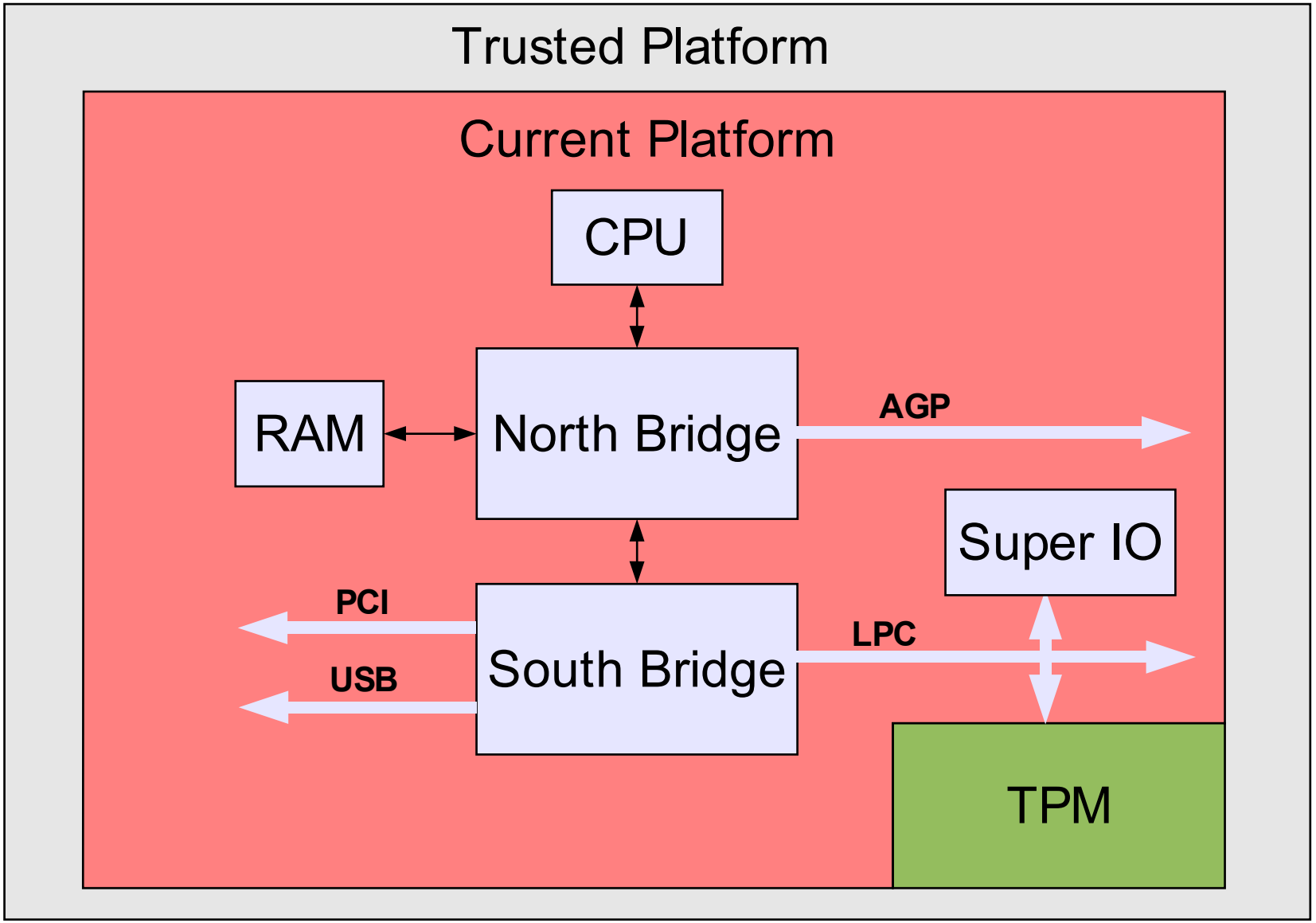
Definitionen

- Trusted Platform := enthält TBB
- TBB = „Trusted Building Block“ := TPM + RTM
- Subsystem := TPM + TSS (+ RTM ?)
- TPM = „Trusted Platform Module“
- TSS = „Trusted Platform Support Services“
- RTM = „Root of Trust for Measurement“
- CTRM = „Core Root of Trust for Measurement“

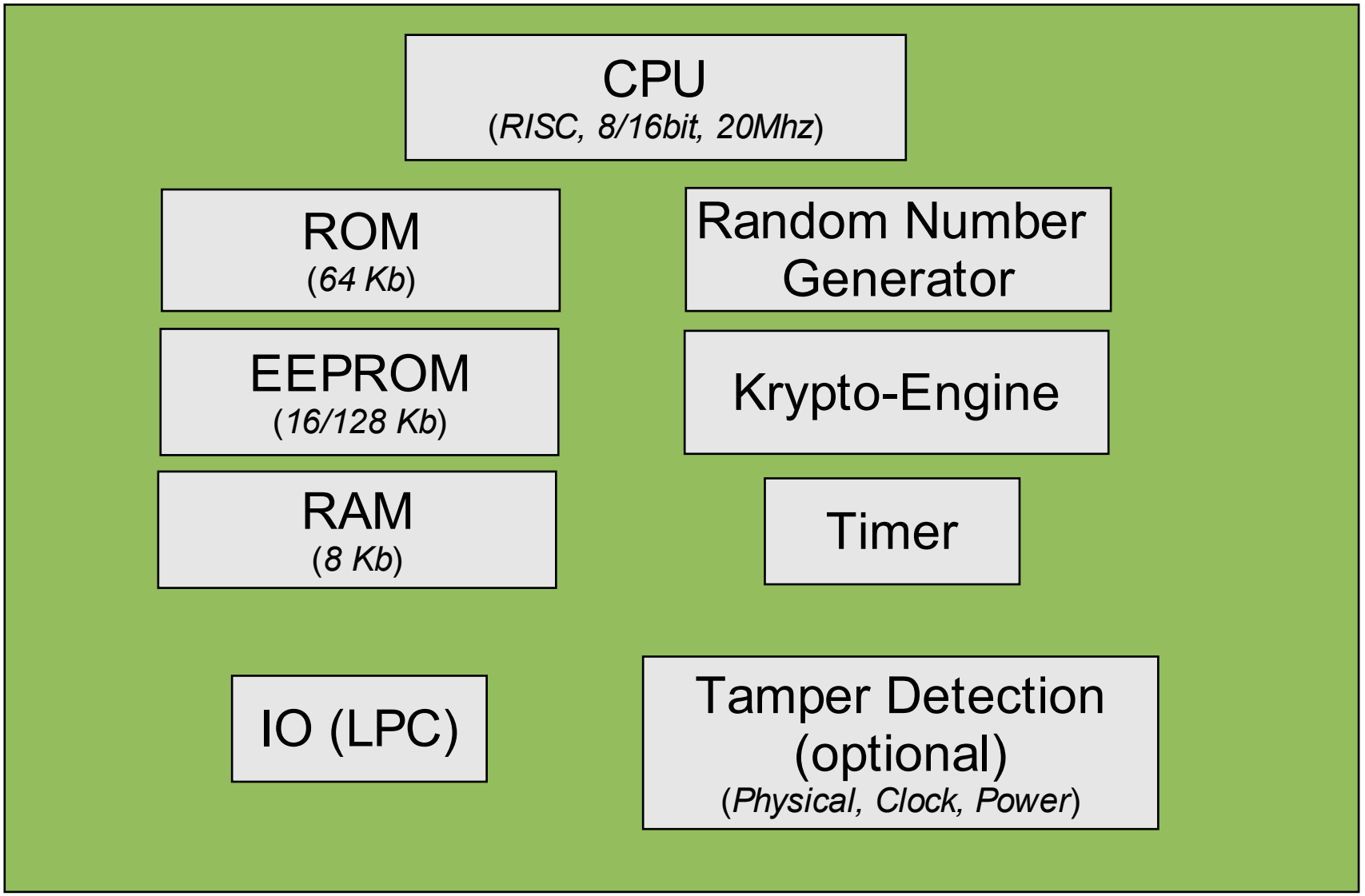
System - Überblick



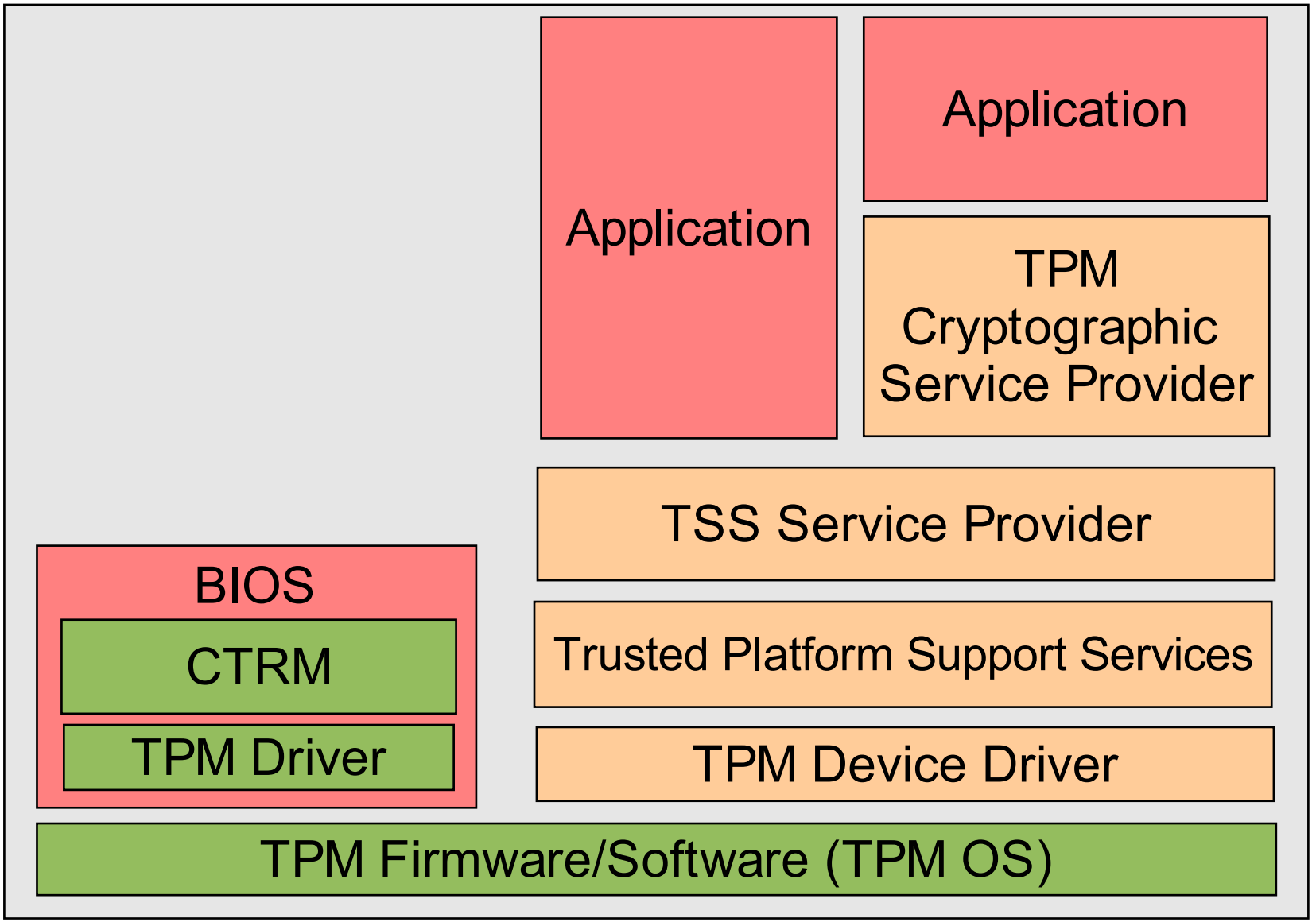
Hardware - Integration



Hardware - TPM



Software - Integration



TPM - Funktionen 1

- Kryptographische Funktionen
  - Zufallszahlengenerator
  - Hashfunktionen (SHA-1, HMAC)
  - Asymmetrische Ver-/Entschlüsselung (RSA)
  - Asymmetrische Schlüsselgenerierung (RSA mit 512, 1024 und 2048 bit)
  - Symmetrische Ver-/Entschlüsselung (3DES) ist NICHT Bestandteil des TPM (aber der TSS)

TPM - Funktionen 2

- Schlüsselspeicherung
- Schlüsselverwaltung
- Selbsttest
- Identifikation und Authentifizierung
- Zugriffskontrollen

TPM - Dienste

- Ermittelung und Schutz der Platform-Integrität (Measurement)
- Geschützter Speicher (Trusted Storage)
- Zustandauskünfte (Reporting)

Integrität

- Ermittelung der Integritätsdaten
  - „Chain of Trust“: Bevor die Kontrolle an die nächste Komponente weitergegeben wird, wird deren aktueller Zustand im TPM gespeichert (als Hashwert oder als Rohdaten)
  - Der CRTM muß immer zuerst die Kontrolle erhalten und speichert nur seine Versionsnummer im TPM
  - Integritätsdaten werden im TPM nicht überschrieben sondern mit den vorherigen Daten verkettet
  - Jeder neu ermittelte Systemzustand kann so auf Übereinstimmung mit einem vorherigen Systemzustand überprüft werden
  - Stimmen bestimmte Zustände nicht überein, werden die entsprechenden TPM-Funktionen deaktiviert

Integrität - Probleme

- Wie werden gewünschte und ungewünschte Systemänderungen unterschieden ?
- Zuverlässigkeit der Integritätsdaten ?
  - „The Core Root of Trust for Measurement (CRTM) MUST be an immutable portion of the Platform's initialization code that executes upon a Platform Reset.
    The trust in the Platform is based on this component. The trust in all measurements is based on the integrity of this component."
  - „In this specification immutable means that in order to maintain trust in the Platform, the replacement or modification of code or data MUST be performed by a Platform manufacturer-approved agent and method."

[Quelle „TCPA PC Specific Implementation Specification" v1.00]

Geschützter Speicher

- Unterstützung für persistente und nicht-persistente Inhalte
- kann Schlüssel, Integritätsdaten, Konfigurationsdaten und Benutzerdaten enthalten
- existiert innerhalb des TPM, um direktes Auslesen zu verhindern („Tamper resistance“ ist aber nur optional)
- Zugriff auf die Daten ist nur über TPM Funktionen möglich. Diese geben die Daten evtl. nur abgesichert weiter (verschlüsselt, signiert).
- Einige Daten sind nur über privilegierte Funktionen zugreifbar, die eine Authenfizierung erfordern.
  Einige Daten können nur TPM-intern genutzt werden.

Geschützter Speicher 2

- Schlüsselspeicher: Unterteilung in „migratable keys“ und „non-migratable keys“
- Schlüsselhierachie:
  - ein Schlüssel schützt alle darunterliegenden (durch verschlüsselte Speicherung)
  - Es gibt verschiedene Schlüsselarten mit unterschiedlichen erlaubten Operationen
  - Sicherheit des „Storage Root Key“ gewährleistet Vertrauen in alle anderen Schlüssel:
    - wird im TPM generiert
    - ist „non-migratable“
    - darf ausschliesslich zur TPM-internen Verschlüsselung anderer Schlüssel verwendet werden

Einige persistente Daten

- Endorsement Key
  - dient zur eindeutigen Identifizierung des TPM (und somit auch des Gesamtsystems)
  - kann nur einmal erzeugt werden (z.B bei der Herstellung) und ist dann nicht mehr änderbar
- Storage Root Key
- Manufacturer's Public Key
  - wird für Maintance-Funktionen benutzt (Übertragung der non-migratable keys auf ein anderes TPM)
- TPME Identity Key (?)
  - keine weitere Erwähnung (verm. weiterer Hersteller-Schlüssel)
- Owner Authorization Data

Speicher - Probleme

- Owner und SRK können zwar gelöscht werden, diese Funktion ist aber deaktivierbar
- Backup / Recovery
    - gespeicherte Inhalte können nur mit dem zum Speichern verwendeten Schlüssel, demselben TPM (bzw. Endorsement Key) und demselben Systemzustand wiederhergestellt werden
    - „non-migratable keys“ können nur durch Kooperation mit dem Hersteller in ein anderes, baugleiches TPM übertragen werden

Allgemeine Probleme

- TPM kann nicht komplett deaktiviert werden
  - Immer aktiv sind:
    - Das Ermitteln und Speichern der Integritätsdaten
    - Statusabfrage des TPM
    - Selbsttest
- Integrität des TPM
  - Es existiert ein Upgrade-Befehl für das TPM, dessen Spezifikation bis auf folgende Bedingungen im wesentlichen Hersteller-spezifisch ist:
    - Herkunft der Upgrade-Informationen muß überprüfbar sein (z.B. digitale Signatur mit Hersteller-Schlüssel)
    - Authorisierung des TPM-Eigentümers ist erforderlich

Allgemeine Probleme 2

- Identitäts-Probleme:
  - „Anonyme Identitäten“ werden mittels „Trusted Third Party“ realisiert.
    Diese kann Identitäten auf das entprechende TPM (bzw. den Endorsement Key) und evtl. auf den Benutzer abbilden.

Fazit

- Vertraulichkeit und Integrität von Daten sowie die Integrität des Computersystems werden durch kryptographische Verfahren gestärkt.
  Die Spezifikationen haben aber Lücken, die Schwächen in der Implementation erlauben.
- Datenschutz-Aspekte werden kaum berücksichtigt.
- Es werden PKI-ähnliche Strukturen genutzt, wichtige Funktionen (backup, key revocation, key recovery) jedoch nicht berücksichtigt.
- „Kryptographische Aufrüstung“ lässt sich auch mit Smartcards verwirklichen
- Abhängigkeit vom Hersteller wird verstärkt

Fazit

- Solide kryptographische Basis oder Marketingschlagwort ?
  - “Digital signatures also prevent the data source from denying that the data was created by the source (a feature known as ‘non-repudiation’).
    If the TCPA-enabled system is digitally signing the contract, the identity used for the signature can be simultaneously reliable and anonymous.“
    [aus „TCPA Security and Internet Business: Vital Issues for IT“]
- Öffentliche Darstellung der TCPA widerspricht den eigenen Zielen
- Das „eigentliche“ Ziel ?
  - Entwurf einer Spezifikation die (zwangsweise) Vertrauen in die Computer-Industrie schafft.
    Aber wozu braucht man dann noch ein sicheres Subsystem ?

Ende

Dieser Vortrag und weiterführende Links:

http://www.michel-messerschmidt.de/de/tcpa.html