

gefördert durch das



Bundesministerium
für Wirtschaft
und Technologie

Trusted Computing

→ Projekte, Erfahrungen und Piloten

Markus Linnemann

Niklas Heibel

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
www.internet-sicherheit.de



Ruhr-Universität Bochum



Fachhochschule
Gelsenkirchen



TECHNISCHE
UNIVERSITÄT
DRESDEN



Sirrix AG
security technologies

escrypt
Embedded Security

EMSCB

European Multilaterally Secure Computing Base
www.emscb.org

Agenda

- ◉ **Problemstellung**
- ◉ **Organisation und Motivation**
- ◉ **Idee und Funktionen**
- ◉ **Trusted Platform Module - Basisfunktionen**
- ◉ **Forschungsprojekte, Piloten und Anwendungen**
- ◉ **Grenzen der TC-Technologie – Vorbehalte**
- ◉ **Fazit**



Trusted Computing

→ Die Problemstellung

- ◉ **Die Bedrohung ist präsent wie nie**
 - Phishing, Spam, Viren, Trojanische Pferde, Würmer, Exploits, ...
 - **das Gefahrenpotenzial hat sich enorm erhöht**
 - ◉ **Anforderungen an die IT heutiger Unternehmen & Institutionen:**
 - Schnelligkeit und Anpassungsfähigkeit
 - Entwicklung zu verteilten Systemen
 - *eGovernment*
 - *ID- und Rechtemanagement auf unterschiedlichen Systemen*
 - *Digital Rights Management*
 - Systeme müssen sicher sein und lange laufen
 - *Schutz der Daten, der Privatsphäre, des Urheberrechts*
- **Anforderung:** Mehr Vertrauenswürdigkeit in IT-Systeme

Trusted Computing

→ Organisation und Motivation

- ◉ **Trusted Computing Group (TCG):**
Industriekonsortium bestehend aus den führenden 170 IT-Firmen (AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony, Sun, ...)
 - Deutsche Beteiligung: Infineon, Giesecke & Devrient, Siemens, Utimaco Safeware, Sirrix AG, ...
- ◉ **Grundmotivation**
 - Entwicklung **offener Spezifikationen** für **vertrauenswürdige IT-Systeme** (Server, PC, eingebettet, usw.)
 - Sicherheit verteilter Anwendungen verbessern
 - Keine massive Veränderung existierender Hard- bzw. Software



Trusted Computing

→ Idee und Funktionen (1/3)

◉ **Idee**

→ Zusammenwirken von **vertrauenswürdigen Hardware- und Software-Sicherheitsmechanismen**

- Manipulationssichere Hardwarekomponente
→ Stärkung gegen Software-basierte Angriffe
- Überprüfung der Integrität und Authentizität von Rechnersystemen auch gegenüber externen Kommunikationspartnern
- Verbesserter Datenschutz und verbesserte Sicherheit beim Aufbewahren und Übertragen von Daten
- Schutz vor Malware (Viren, Würmer, Trojaner, ...)

→ **Verhält sich ein Rechnersystem für eine spezielle Aufgabe so, wie es erwartet wird, dann gilt das Rechnersystem als vertrauenswürdig.**

Trusted Computing

→ Idee und Funktionen (2/3)

- ◉ **Überprüfbares Booten**
 - Systemkonfiguration kann mittels eines persönlichen Gerätes (Smartcard, USB-Stick, Handy, ...) überprüft werden
- ◉ **Sealing (Versiegeln)**
 - Kryptographische Schlüssel können an das IT-System und/oder eine bestimmte Softwarekonfiguration gebunden werden
 - Schutz vor Manipulationen des Betriebssystems
- ◉ **Attestation (Attestierung)**
 - Aktuelle Softwarekonfiguration des IT-Systems wird dargestellt
- ◉ **Remote Attestation**
 - Erkennung manipulierter IT-Systeme
 - Kommunikation nur mit vertrauenswürdigen IT-Systemen

Trusted Computing

→ Idee und Funktionen (3/3)

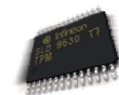
◉ **Sicherer Speicher**

- Speicherung kryptographischer Schlüssel im Hardwaremodul
- Erzeugung sicherer kryptographischer Schlüssel

◉ **Access Control & Digital Rights Enforcement**

- Durchsetzung von (Zugriffs-)regeln in einem Netzwerk mit unbekanntem IT-Systemen (TNC)

→ Weitere Spezifikationen der TCG sind in Bearbeitung



TPM

Trusted Computing

→ Trusted Platform Module (TPM)

◉ **Funktionen des TPM - Version 1.1b und 1.2**

- Sicherer Zufallsgenerator (sichere kryptographische Schlüssel)
- Kryptographische Funktionen: Signatur (RSA), Hash (SHA-1)
- Erzeugung verschiedener kryptographischer Schlüssel
- Platform Configuration Register (PCR) → Zur Speicherung der Plattformkonfiguration

→ Das TPM entspricht im Prinzip einer fest eingebauten SmartCard, die **an ein Rechnersystem gebunden ist**, wie z.B. PC, Notebook, PDA, Drucker, Router, Kühlschrank usw.

◉ **Verbreitung von TPMs**

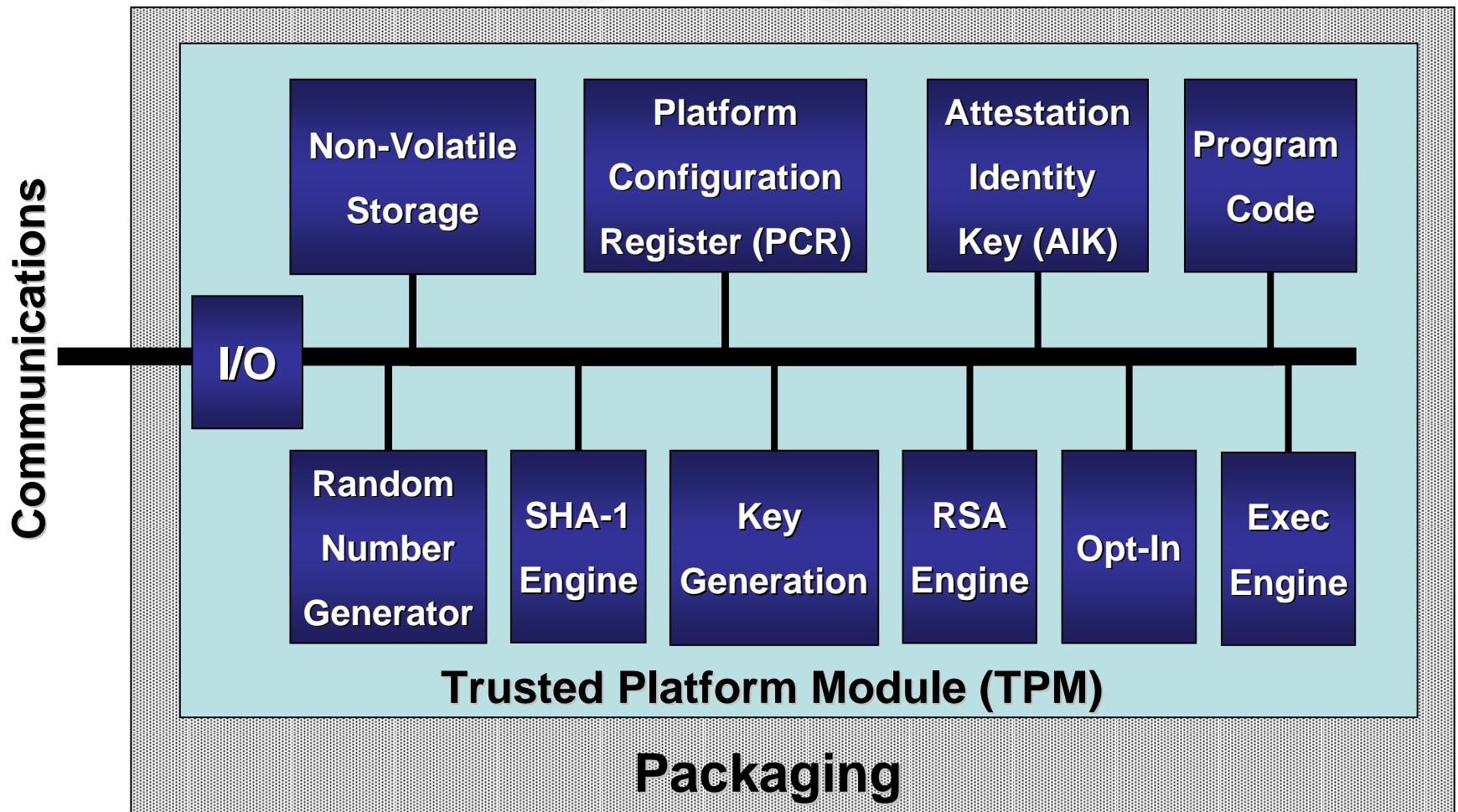
- 60 Millionen bis Ende 2006
- 130 Millionen bis Ende 2007
- 200 Millionen bis Ende 2008



TPM

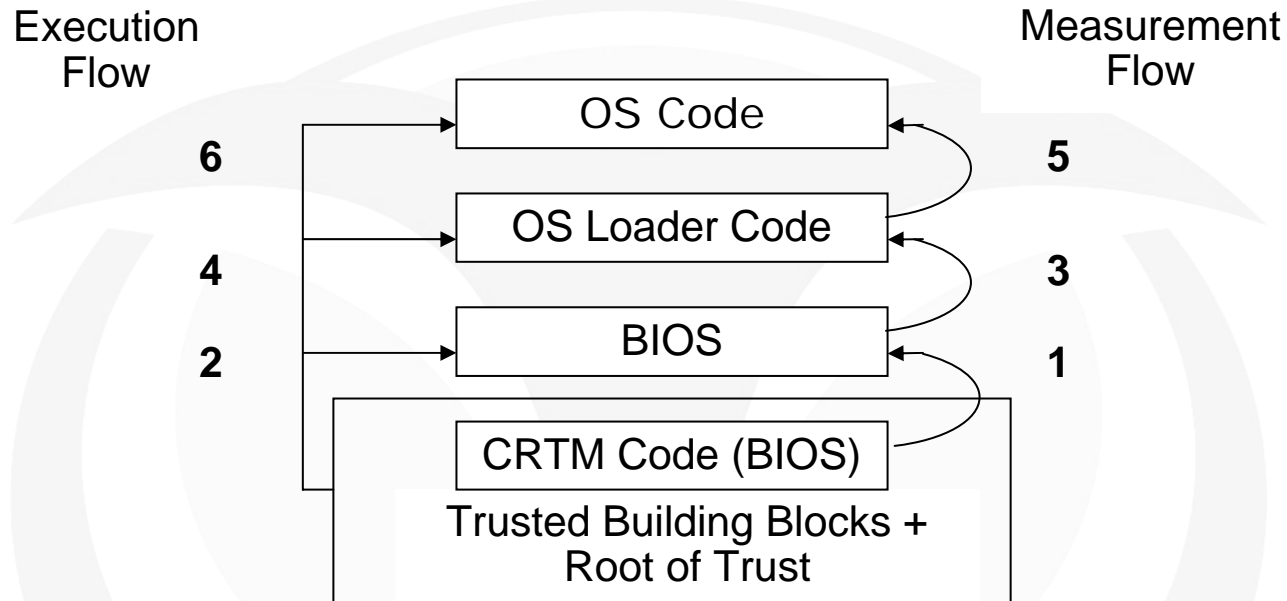
Trusted Computing

→ Basisfunktionen TPM



Trusted Computing

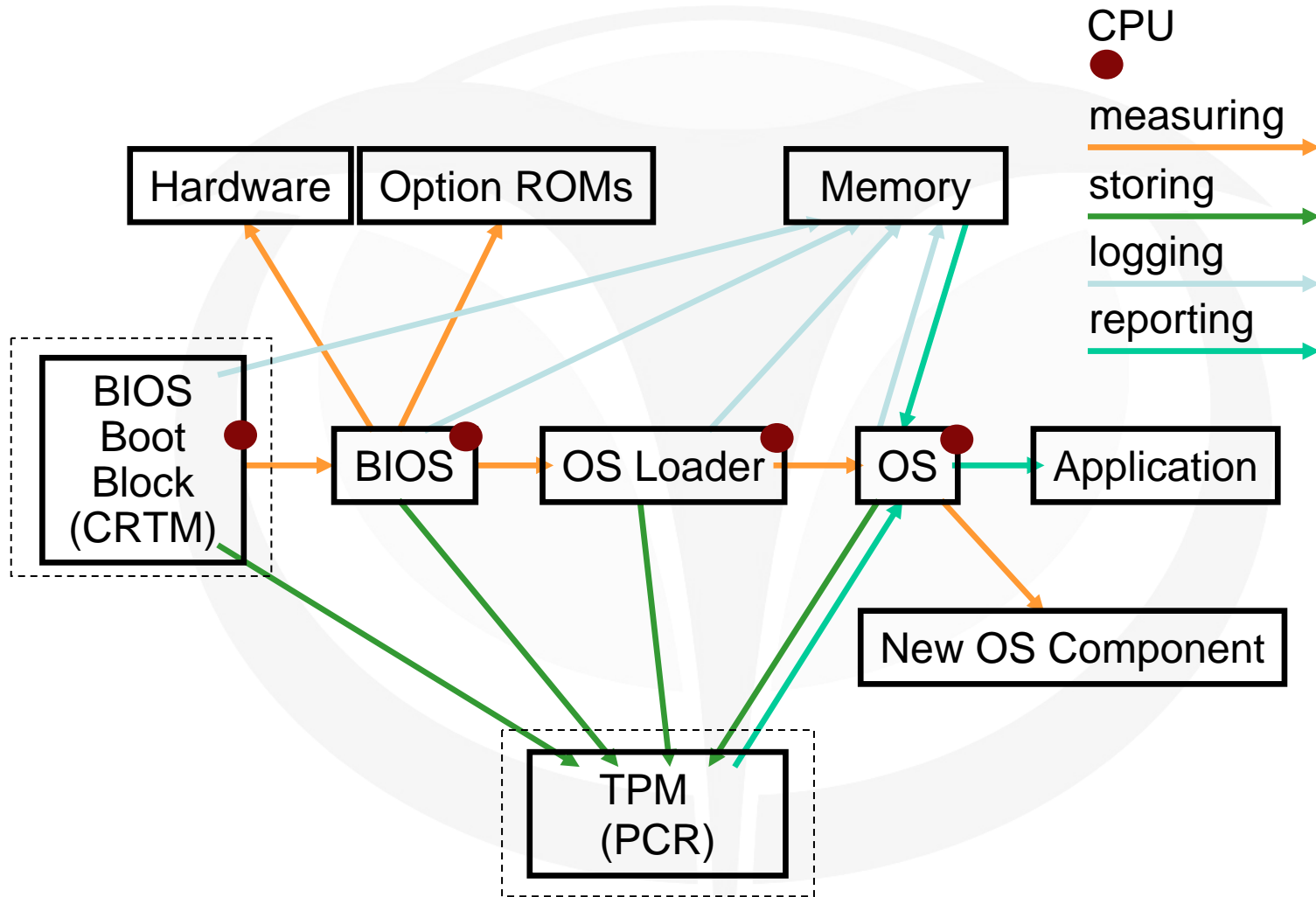
→ Trusted Boot (1/2)



- Beim Trusted Boot wird der Root of Trust gebildet, in dem sich die einzelnen Komponenten aufeinander aufbauend messen.
- CRTM (Core Root of Trust Measurement) muss „read only“ sein! (steht im EPROM oder im TPM)
- Jede Komponente wird gemessen bevor sie geladen wird.

Trusted Computing

→ Trusted Boot (2/2)



(C) 2005 by European Multilaterally Secure Computing Base Consortium

Forschungsprojekte

→ Europa und Co

◉ **EMSCB**

- **Ziel:** Entwicklung einer Sicherheitsplattform und Schaffung eines offenen Standards
- Entwicklungsprojekt mit "festen" Ergebnissen (Piloten)
- Best Practice des OTC-Projekts

◉ **OTC**

- **Ziel:** Entwicklung eines offenen TC Frameworks
- Forschungsprojekt auf Open Source Basis
- Behandlung unterschiedlicher Virtualisierungskonzepte

◉ **Weitere Projekte:**

- Projekt in Neuseeland
- Projekt in Japan

Piloten & Anwendungen

→ TC-Technologie in aktuellen Systemen

- ◉ **Konforme Systeme mit TPM**
 - Dell, Fujitsu Siemens, HP und IBM
- ◉ **Verfügbare Applikationen**
 - Turaya, RSA Secure ID, Checkpoint VPN, Verisign PTA, ...
 - Software von IBM
 - Windows: verändertes Login, rudimentäre Verschlüsselungswerkzeuge
 - Linux: Testpaket (samt Quellen) mit Kernel-Modul, Bibliothek, API und Beispielprogrammen
- ◉ **Microsoft**
 - BitLocker
 - Festplattenverschlüsselung (optional in MS Vista)

Trusted Computing Group

→ Grenzen der TC-Technologie

- ◉ ***Keine Lösung für typische Entwicklungsfehler***
 - Bugs in Software, Buffer Overflows, Angriffe gegen kryptographische Verfahren
 - ◉ ***Kein vertrauenswürdiger Pfad zu Applikationen***
 - Kein Schutz vor Trojanern
 - Keine sichere Benutzer Ein-/Ausgabe
 - ◉ ***Keine Isolation der Anwendungen voneinander***
 - Kein Schutz vor Viren (Anwendungen können aufeinander zugreifen und sich damit gegenseitig infizieren)
- **TPM kann Sicherheitsprobleme existierender Betriebssysteme nicht lösen, kann diese jedoch überprüfen.**
- **Zur Lösung dieser Probleme wird eine Sicherheitsarchitektur benötigt**

Trusted Computing

→ Fazit

Gegenüber herkömmlichen Systemen bietet Trusted Computing

- mehr Sicherheit und
- höhere Vertrauenswürdigkeit,

durch

- die Möglichkeit zur Authentifizierung eines Systems
- die Überprüfbarkeit der Integrität eines Systems
- die Darstellbarkeit der Authentizität und Integrität gegenüber dem eigenen und entfernten Systemen
- den nachweisbaren Bootvorgang ("Trusted Boot")

→ Entscheidend ist die richtige Anwendung der Technologie

Trusted Computing Group

→ Vorbehalte und Befürchtungen gegen TC

- ◉ **Mögliche Einschränkung der Interoperabilität**
 - Binden von Dokumenten/Daten an SW-Konfigurationen
 - Bsp: Keine Word-Dokumente mit OpenOffice
 - Bsp: Keine Windows-Dokumente mit Linux
- ◉ **Monopolbildung & -ausbau möglich**
 - Dokumentenformate werden verschlüsselt
- ◉ **Diskriminierung von Software-Alternativen (Open-Source)**
 - Dokumentenformate werden verschlüsselt
- ◉ **Datenschutz-Verletzungen**
 - Herausgabe genauer Informationen über ein IT-System
- ◉ **Probleme durch zu restriktive Lizenzpolitiken**
 - Lizenzen werden an TPM gebunden
- ◉ **Fragwürdige Vertrauenswürdigkeit**
 - Closed Source, kein Re-Engineering

gefördert durch das



Bundesministerium
für Wirtschaft
und Technologie

Trusted Computing zum Schutz von Daten, Kommunikation, Privatsphäre, Urheberrecht: Entscheidend ist die richtige Anwendung der Technologie!

www.emscb.de

Markus Linnemann

Niklas Heibel

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
www.internet-sicherheit.de

EMSCB

European Multilaterally Secure Computing Base
www.emscb.org