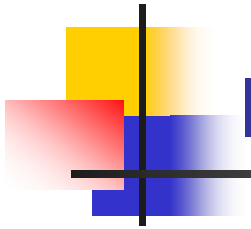
# Trusted Computing Group (TCG) Teil 1

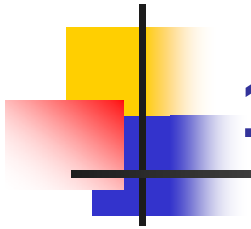
Xin , Hai

200120039



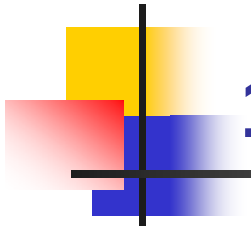
# Inhalt

- 1. Wofür steht Trusted Computing?
- 2. Sicherheitsaspekte in der TCG Spezifikation
- 3. Wie funktioniert es?
- 4. Befürchtungen der Kritiker
- 5. Position des Bundes
- 6. Fazit
- 7. Literatur



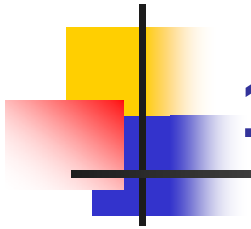
# 1.Wofür steht Trusted Computing? (1)

- Die Trusted Computing Group (TCG) ist die Nachfolgeorganisation einer Allianz von Microsoft, Intel, IBM, HP und AMD, die einen Standard für 'sicherere' PC fördern will. Ihre Definition von 'Sicherheit' ist allerdings umstritten; nach deren Spezifikationen gebaute Computer werden für die Software- und Inhalteanbieter vertrauenswürdiger sein für die Anwender allerdings eher weniger.



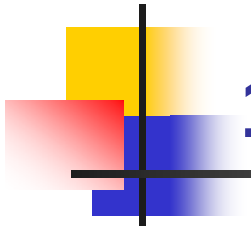
# 1.Wofür steht Trusted Computing? (2)

- IBM ---- 'Trusted Computing'
- Microsoft ---- 'trustworthy computing' (vertrauenswürdiger Computereinsatz)
- Die Free Software Foundation ---- 'treacherous computing' (verräterischer Computereinsatz)



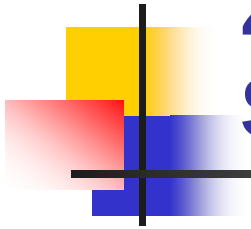
# 1.Wofür steht Trusted Computing? (3)

- Geläufig war einige Zeit auch der Name TCPA (Trusted Computing Platform Alliance). Das war der frühere Name der TCG vor ihrem Zusammenschluss als eigenständige Firma.
- Die Softwareimplementation, der TCG-Spezifikation, die in der nächsten Windows-Version das Trusted Computing ermöglichen soll heißt inzwischen NGSCB.
- Viele Beobachter gehen davon aus, dass diese Namensverwirrung beabsichtigt ist - die Mitglieder wollen davon ablenken, was TC wirklich ausmacht.



# 1.Wofür steht Trusted Computing? (4)

- Das erklärte Ziel der Trusted Computing Group ist es, Rechner sicherer zu machen. Das umfasst den Schutz vor Viren, die eindeutige Identifikation in vernetzten Systemen und betrifft auch das Digital Rights Management, kurz DRM, also das Verhindern der Erstellung von illegalen Kopien und Vervielfältigungen.



# 2.Sicherheitsaspekte in der TCG Spezifikation (1)

- Der TCG Ansatz ergibt neue Systemstrukturen: Während bisher Sicherheit durch zusätzliche Verschlüsselungsebenen oder Anti-Virus Software erreicht werden sollte, beginnt TCG bereits auf der untersten Ebene der Plattform.

- Es greift aktiv in den Bootvorgang eines Rechners ein.

# 2.Sicherheitsaspekte in der TCG Spezifikation (2)

- Alles basiert auf dem Trusted Platform Module. Das ist ein HW-Baustein, der direkt auf dem Mainboard angebracht wird. Von dieser untersten Schicht wird beim Systemstart eine ununterbrochene Sicherheitskette („ Chain of Trust “) bis zu den Applikationen hochgezogen.

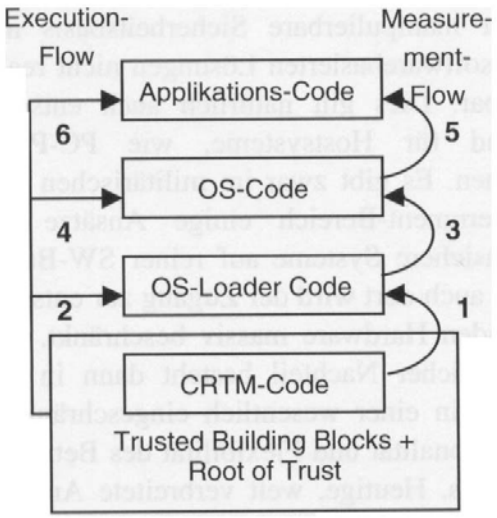
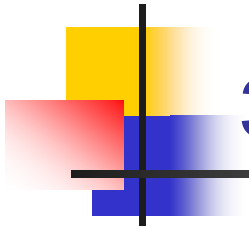
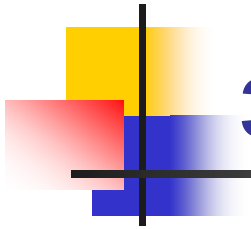



Abb. 1: Aufbau der „Chain of Trust“



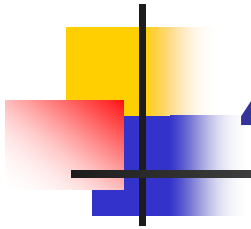
# 3. Wie funktioniert es? (1)

- TC sorgt für den Einbau einer Überwachungs- und Meldekomponente in künftige PCs. Die bevorzugte Variante in der ersten Phase der Einführung ist ein "Fritz"-Chip - ein Smartcard-Chip oder Dongle, der aufs Motherboard gelötet wird.
- Die aktuelle Version des Fritz-Chip hat eine passive Überwachungskomponente, die den Hash-Wert der Maschine beim Hochfahren speichert.
- Der Security Kernel des Betriebssystems (der 'Nexus') überbrückt die Lücke zwischen dem Fritz- Chip und den Sicherheitskomponenten der Anwendungen (den 'NCAs').



# 3. Wie funktioniert es? (2)

- Sobald sich der Rechner in diesem Zustand befindet, mit einer TC-konformen Anwendung im Speicher, die gegenüber Einmischung anderer Software geschützt ist, kann Fritz Inhalte für Dritte zertifizieren; z.B. wird Disney per Authentifizierungsprotokoll versichert, dass der Rechner ein geeigneter Empfänger von "Schneewittchen" ist.
- Der Disney Server sendet daraufhin die verschlüsselten Inhalte mit einem Schlüssel, den der Fritz-Chip zur Entschlüsselung derselben verwendet.
- Das bedeutet, dass Disney seine Inhalte nur für solche Media Player freigeben kann, deren Hersteller sich zur Durchsetzung gewisser Bedingungen bereit erklären.

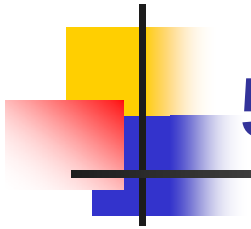


# 4. Befürchtungen der Kritiker (1)

- TC bildet eine Computerplattform, die verhindert, dass der Anwender die darauf laufenden Anwendungen manipulieren kann, welche abgesichert mit dem Programmhersteller und untereinander kommunizieren können.
- TC wird es zudem viel schwieriger machen, nicht lizensierte Software zu nutzen.
- Die nun vorgeschlagenen Mechanismen sind allerdings etwas subtiler.

# 4. Befürchtungen der Kritiker (2)

- Es gibt vielerlei Möglichkeiten.
- Es gibt natürlich auch Nachteile.
- Allgemein gilt, dass mit TC-kompatiblen Systemen erstellte digitale Objekte - egal auf welchen Systemen sie sich befinden - weiterhin der Kontrolle des jeweiligen Autors unterstehen und nicht dem Besitzer des Systems, so wie es momentan noch der Fall ist.



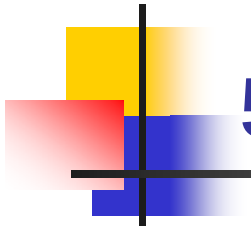
# 5. Position des Bundes (1)

- Ende 2003 hat das Bundesministerium des Innern (BMI) gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesbeauftragten für den Datenschutz (BfD) und dem Bundesministerium für Wirtschaft und Arbeit (BMWA) eine offizielle Stellungnahme der Bundesregierung zu Trusted Computing erarbeitet, in der folgende Anforderungen an die TCG formuliert sind:

# 5. Position des Bundes (2)

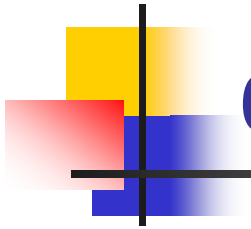
- Transparenz der Entwicklungsarbeiten in der TCG unter Berücksichtigung deutscher Sicherheitsinteressen
- Zeitnahe Bereitstellung von Informationen, die insbesondere auch Nicht-Mitgliedern bei der TCG sowie Entwicklern von Open-Source-Software zur Verfügung stehen
- Berücksichtigung von Anforderungen des Datenschutzes in Deutschland.

Die Stellungnahme des Bundes zu Trusted Computing kann unter der Webadresse www.bsi.bund.de/trustcomp/index.htm abgerufen werden.



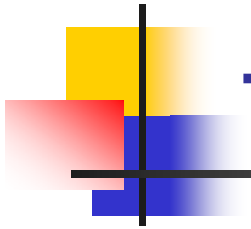
# 5. Position des Bundes (3)

- Im BSI wurde eine Arbeitsgruppe eingerichtet, die die technische Bewertung der Tätigkeiten bei TCG vornimmt und das BMI regelmäßig unterrichtet.
- Das Konzept der TCG besitzt das Potential, für mehr Computersicherheit zu sorgen, da es auf hardwarebasierten Schutzmechanismen beruht.



# 6. Fazit

- Trusted Computing ist eine Chance, die Sicherheit vernetzter PC nachhaltig zu erhöhen. Voraussetzung für den Erflog des TCG-Konzeptes ist das Vertrauen der Anwender. Angesichts der technischen Komplexität des Konzepts und der theoretischen Missbrauchsmöglichkeiten der Technologie wird das Vertrauen nicht leicht zu erringen sein. Die Bundesregierung verfolgt die Entwicklungen in der Trusted Computing Group intensiv. Das Ziel des Bundes ist eine wirksame und für die Anwender akzeptable Ausgestaltung der neuen Technologie.



# 7. Literatur


- Ross Anderson : Trusted Computing FAQ 1.1 2003
- Balacheff, Chen,  Pearson, Plaquin, Proudler: Trusted Computing Platforms, HewlettPackard Books, 2003
- Hans Brandl , Thomas Rosteck:  Technik, Implementierung und Anwendung des Trusted Computing Group-Standards (TCG)

# Vielen Dank!