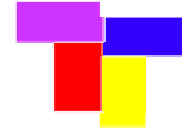


„Trusted Computing“ kontrolliertes Vertrauen

Clemens Brandt
Andreas Hinnerichs
Jörn Hoffmann

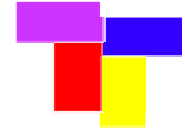
Vortrag in der LV Information Rules 1
WS 2003/2004

17.12.2003



Überblick

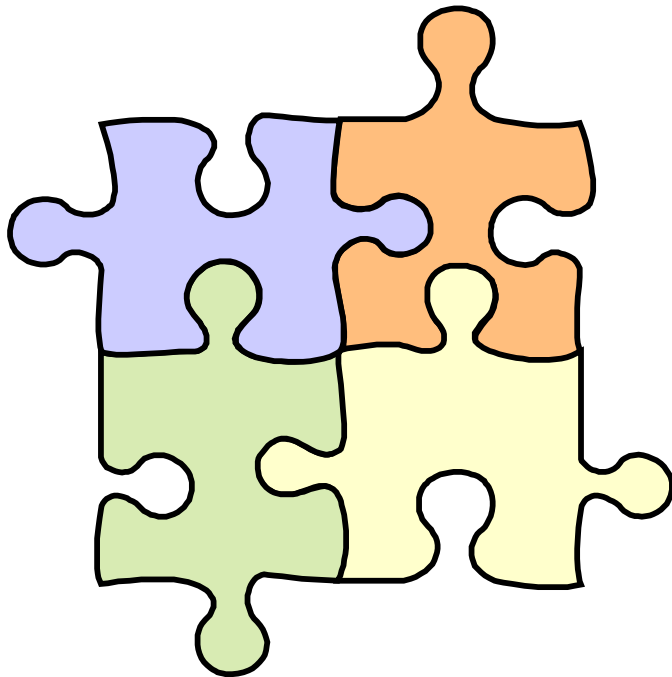
- „Trusted Computing“ –
die Idee, die Technik, die Geschichte
- „Trusted Computing Group“ –
Kontrollmöglichkeiten und Folgen
- Recht und Politik
- Unsere Meinung
- Diskussion



Die Idee hinter „Trusted Computing“

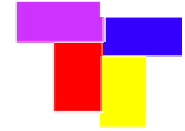
- Plattformübergreifender Standard
- Vor Software-Angriffen (Trojaner, Viren) schützen
- Hardware-Modifikationen (Änderung der Systemkonfiguration) ausschließen
- Daten vor unberechtigtem Zugriff schützen

Was ist TC technisch?



4 Komponenten

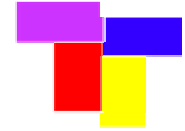
- Hardware (Fritz-Chip/TPM)
- Abgesicherter Speicher
- Mehrere Sicherheitskernel
- Ein Netz von öffentlichen Onlineservern



Geschichte der TCPA

- 11. Oktober 1999:
Gründung der "Trusted Computing Platform Alliance" (TCPA) durch Compaq, HP, IBM, Intel und Microsoft
- Über 200 Mitglieder bis April 2003

Jedes Mitglied hat eine Stimme und Vetorecht
Entscheidungen nur einstimmig

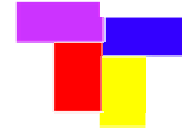


Geschichte der TCG

- 8. April 2003:
Gründung der "Trusted Computing Group" (TCG)
- Offizieller Nachfolger der TCPA

verschiedene Mitgliedsklassen
(Promoter, Contributor, Adopter)
Entscheidungen mit einer 2/3-Mehrheit

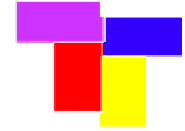
Namensänderung wegen zu negativer Publicity?



- **Promoters**
AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony, Sun
- **Contributors**
Agere Systems, ARM, ATI, Atmel, Broadcom, Comodo, Fujitsu, Siemens, Gemplus, Infineon, Legend Limited Group, National Semiconductor, Nokia, NTRU Cryptosystems, NVIDIA, Philips, Phoenix, Rainbow Technologies, RSA Security, SCM Microsystems, Seagate, Shang Hai Wellhope, Silicon Storage, Standard Microsystems, STMicroelectronics, Texas Instruments, Utimaco Safeware, VeriSign, Wave Systems
- **Adopters**
Ali Corporation, American Megatrends, AuthenTec, Gateway, M-Systems Flash Disk Pioneers, Silicon Integrated Systems, Softex, Toshiba, Winbond Electronics

Auswirkungen auf die Computerbenutzung

- TC ist an-/abschaltbar
- TC Dokumente sind nur von TC Software nutzbar
- Software ist nur dann ausführbar, wenn sie bezahlt wurde
- Modifikationen an Software wird verhindert
- Urheber und natürlich Softwarehersteller haben volle Kontrolle über erstellte Dokumente: Von wem werden sie benutzt, wie lange, usw.
- Hintertüren sind möglich

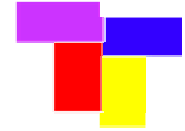


Wieso sollte die TCG so weit gehen?

- Die Frage ist eher:
Wieso sollte die TCG nicht so weit gehen?
- Schutz für den Anwender oder vor dem Anwender?
- Microsoft, Intel, IBM haben schon mit der Integration begonnen (Palladium/NGSCB, LaGrande, Thinkpad)

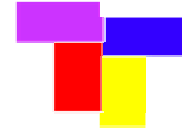
It's a funny thing, we came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains

Bill Gates, zitiert nach Steven Levy



Folgen für die Wirtschaft

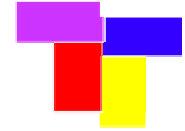
- Für Unternehmen wird der Wechsel von Softwareprodukten erheblich erschwert
- Neben den bisherigen Kosten (Installation, Umschulung, Konvertierungen) kommen neue hinzu: Zertifizierung der alten Dokumente
- Folge: Noch größere Vormachtstellung und Kontrolle von Microsoft und Co.



Folgen für die IT Landschaft

Kleine und mittelständische Unternehmen können an der TC Entwicklung kaum teilhaben, da ohne TCG Mitgliedschaft

- kein Einfluss auf die Standardisierung möglich ist.
- Spezifikationen nur mit zeitlichem Rückstand umgesetzt werden können.
- Spezifikation zwar offen sind – Patente jedoch bei der TCG und deren Mitglieder liegen!

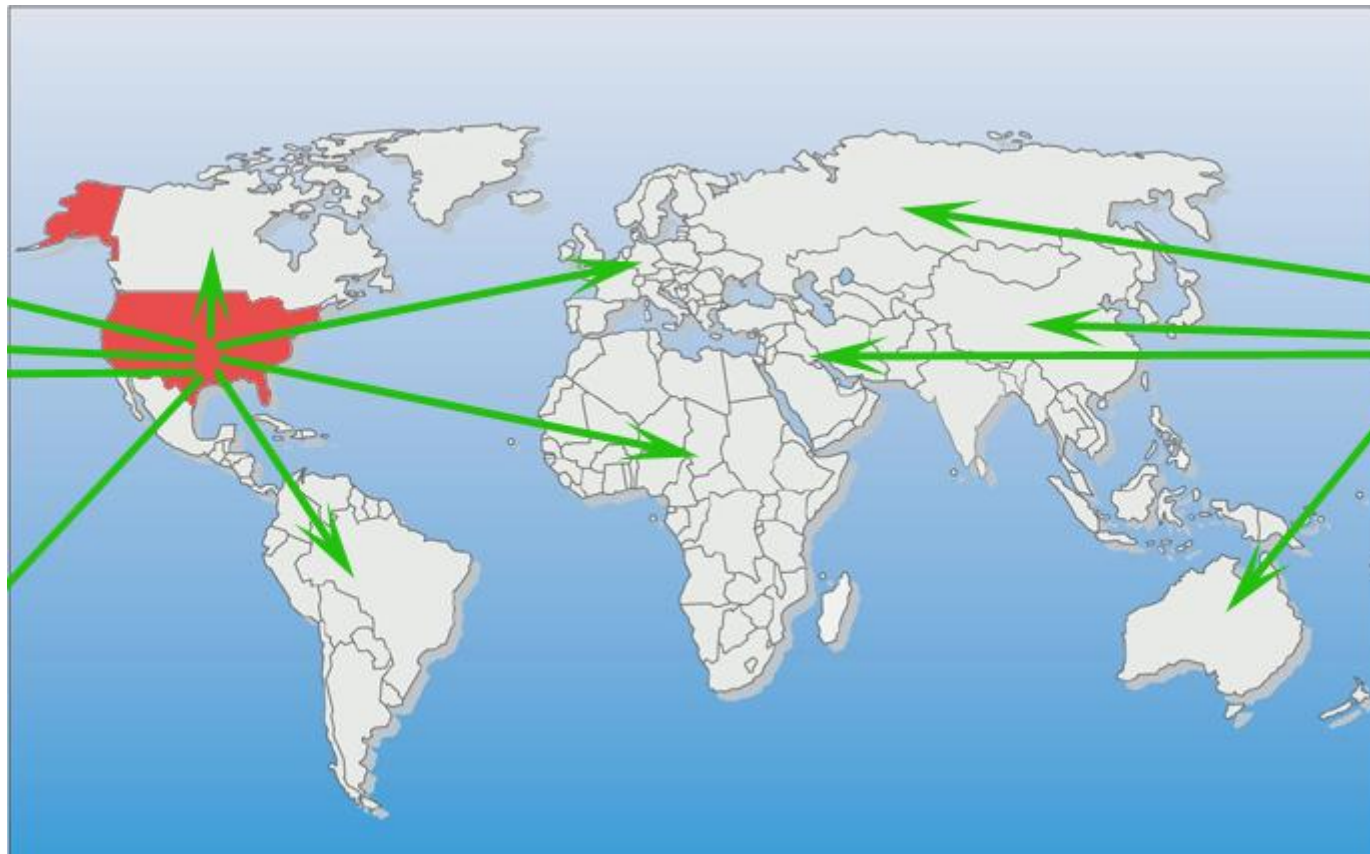


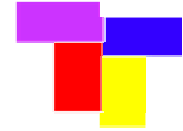
Weitere Folgen

- Innovationskraft wird gehemmt:
 - Wie entstehen Innovationen?
Aus bestehenden Dingen etwas Neues kreieren
 - Mit TC kann keine Software mehr angefasst werden (Samba wäre z. B. niemals zustande gekommen)
- OpenSource nur noch eingeschränkt möglich:
Es muss alles zertifiziert werden (höhere Kosten und mehr Bürokratie)

Folgen für Europa

- Wirtschaftliche Vormachtstellung der TCG Mitglieder, v. a. der Promoter (hauptsächlich amerikanische Unternehmen)
- Unklar: Organisation der Kontrollinstanzen (Kontrolle wird aber überwiegend in amerikanischer Hand sein)
- Folge: Europa wird wirtschaftlich (noch mehr) durch Amerika kontrolliert





Rechtliche Schranken

Amerika

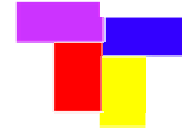
- Es ist in Planung, Gesetze an TCG anzupassen
- Gesetzentwurf schreibt TCG-konforme Geräte vor (bis zu 5 Jahren Gefängnis und 500.000 \$ Geldstrafe)



Europa (Deutschland)

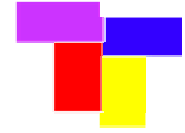
- Pläne der TCG kollidieren mit aktuellen Gesetzen (z. B. Datenschutz)
- Aber: Wo kein Kläger, da auch kein Angeklagter





Politische Aspekte

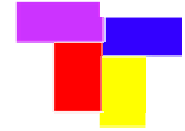
- Abhängigkeit/Kontrolle durch die USA
- Keine Möglichkeit der Kontrolle der Übertragenen Daten (Verschlüsselung)
- Was passiert beim Krisenfall?



Unsere Meinung

- Entwicklung ist negativ und gefährlich
- Ausweg: Europa muss gegenhalten, evtl. mit Partnern aus dem Rest der Welt
- Ziel: Umgestaltung der TCG als öffentliche Zusammensetzung aus Verbänden, Parteien, der Wirtschaft, etc.
- Europa muss stärker auf OpenSource setzen und damit eine Macht gegen die TCG bilden

Politiker und Öffentlichkeit müssen sensibilisiert und mobilisiert werden



Anregungen zur Diskussion

- Akute Bedrohung für jeden Anwender?
- Chance zur Verbesserung der PC-Sicherheit?
- Vielleicht wollen manche Anwender ja TC?
- TCG - die richtige Lösung?