

Trusted Computing

TC/TCG/TCPA/Palladium/NGSCB/LaGrande

**Computer and Internet gave you Freedom.
TCPA would take your Freedom**

- **Die Technologie**
- **Die Auswirkungen**
- **Sonstiges**

**Computer and Internet gave you Freedom.
TCPA would take your Freedom**

- **TCPA – Die Technologie**

- **Wofür steht TC?**
- **Was bringt TC?**
- **Woher kam die Idee?**
- **Wie funktioniert es?**
 - **Woher kommt die Bezeichnung “Fritz-Chip”?**
 - **Wozu kann TC noch verwendet werden?**
 - **Kann TC nicht geknackt werden?**
 - **Wie kann TC missbraucht werden?**
 - **Kann man TC nicht einfach abschalten?**

Wofür steht TC?

- **Trusted Computing Group (TCG) 1999**

Gegründet von:

- **Microsoft**
- **Intel**
- **IBM**
- **HP**
- **Compaq**

Bis heute schon 200 Unternehmen, darunter:

**Adobe, AMD, Fujitsu-Siemens, Gateway, Motorola,
Samsung, Toshiba,....**

**IBM liefert schon die ersten Desktop-PCs und Notebooks mit
TPM (Trusted Platform Module) aus**

Trusted Computing Group (TCG)

- **Trusted Computing**
 - IBM -
- **Trustworthy Computing**
 - Microsoft - (Vertrauenswürdiger Computereinsatz)
- **Palladium**
 - Microsofts vorherige Bezeichnung für die Softwareimplementation im nächsten Windows
- **NGSCB**
 - Nachfolger von Palladium, Next-generation Secure Computing Base
- **LaGrande**
 - Intels Umsetzung von TC – Sichert Arbeits- und Grafikspeicher.
 - Führt einen Trusted Mode für Prozessoren ein. (Beginnend mit Prescott)
 - Erweitert den USB-Bus um einen sicheren Kanal

Was bringt TC? Vorteile!?

- Eine Computeplattform die verhindert, dass der Anwender die darauf laufenden Anwendungen manipulieren kann, welche abgesichert mit dem Programmhersteller und untereinander kommunizieren können.
- Digital Rights Management (DRM)
- Die Musikindustrie kann Musikdownloads verkaufen, die nicht mit anderen getauscht werden können.
- Auktions-Sites könnten auf vertrauenswürdiger Proxy-Software zur Abgabe von Angeboten bestehen, so das ein taktisches Bieten von Bietagenten oder ähnliches nicht mehr Möglich wäre.
- **TC wird es schwieriger machen, nicht lizenzierte Software zu nutzen.**
- **TC wird die Registrierungsprozeduren der Softwareprogramme schützen, so das nicht lizenzierte Software aus dem neuen Ökosystem ausgeschlossen wird.**
- **TC wird es erleichtern Software zu vermieten statt sie zu verkaufen.**
- **Regierungen könnten nur solche Systeme einsetzen, auf denen alle Word-Dokumente, die auf Beamten-PCs erstellt wurden als “klassifiziert” und nicht mehr digital weitergegeben werden könnten.**
- **Die Benutzung von Cheats bei Computerspielen könnte erschwert werden**

Was bringt TC? Nachteile!?

- TC wird die ferngesteuerte Zensur ermöglichen.
- In der simpelsten Form könnten Anwendungen dazu dienen, ferngesteuert, raubkopierte MP3s zu löschen.
- “Traitor Tracing”
- Mit TC-kompatible Systemen erstellte digitale Objekte ermöglichen es – egal auf welchen Systemen sie sich befinden – weiterhin der Kontrolle des jeweiligen Autors unterstehen zu sein und nicht dem Besitzer des Systems, so wie es momentan noch der Fall ist.
- So könnte ein Gericht den Autor eines als verleumderisch eingestuften Dokumentes zur Löschung zwingen – oder den Hersteller der Textverarbeitung, falls sich der Autor weigert.
- Bei solchen Anwendungsmöglichkeiten ist davon auszugehen, dass TC dazu eingesetzt werden wird alles von Pornographie bis zu kritischen Schriften über Politiker zu zensieren.
- Nachteilig für Unternehmen ist, dass die Softwarefirmen den Wechsel auf Produkte eines Mitbewerbers erschweren können.

Woher kam die Idee?

- Das TC Konzept, nachdem ein Rechner in einem definierten Zustand gebooted wird, ist schon in den frühesten Rechnern vorhanden, wo das ROM sich im BIOS befand, und es noch keine Festplatten gab, die ein Virus hätte befallen können.
- “A Secure and Reliable Bootstrap” von Bill Arbaugh, David Farber und Jonathan Smith im Rahmen des “*IEEE Symposium on Security and Privacy*” (1997)
- *US-Patend No. 6,185,678, February 6th, 2001*
- *TrustedNo. 1 Processor von Markus Kuhn*
- *James Anderson, 1972*

Woher kommt die Bezeichnung “Fritz-Chip”?

● Fritz Hollings

- Senator von South Carolina
- TC zwingend für sämtliche Konsumelektronik vorzuschreiben
- 2004 in Rente

Wie funktioniert es?

- Fritz-Chip
- Abgeschirmter Bereich im Speicher
- Sicherheitskernel im Betriebssystem
 - Von Microsoft “Nessus” genannt
- Sicherheitskernel in jeder TC Anwendung
 - Von Microsoft “NCA” genannt
- Eine Infrastruktur von Onlineservern, die von Hardware- und Softwareherstellern betrieben werden um das Ganze miteinander zu verbinden

Wie funktioniert es?

Fritz Chip

Überwachte den Bootprozess, so das der PC in einem vorgesehenen Zustand mit bekannter Hard- und Software hochfuhr.

Fritz Chip

Passive
Überwachungs-
komponente

Speichert den Hash-Wert der Maschine (bestehend aus den einzelnen Details der Hardware (Soundkarte, Grafikkarte, etc.) und der Software (Betriebssystem, Treiber, usw.)

Wie funktioniert es?

Fritz-Chip

Hash (2048bit) 

Betriebssystem

Nexus

Kryptographische
Schlüssel

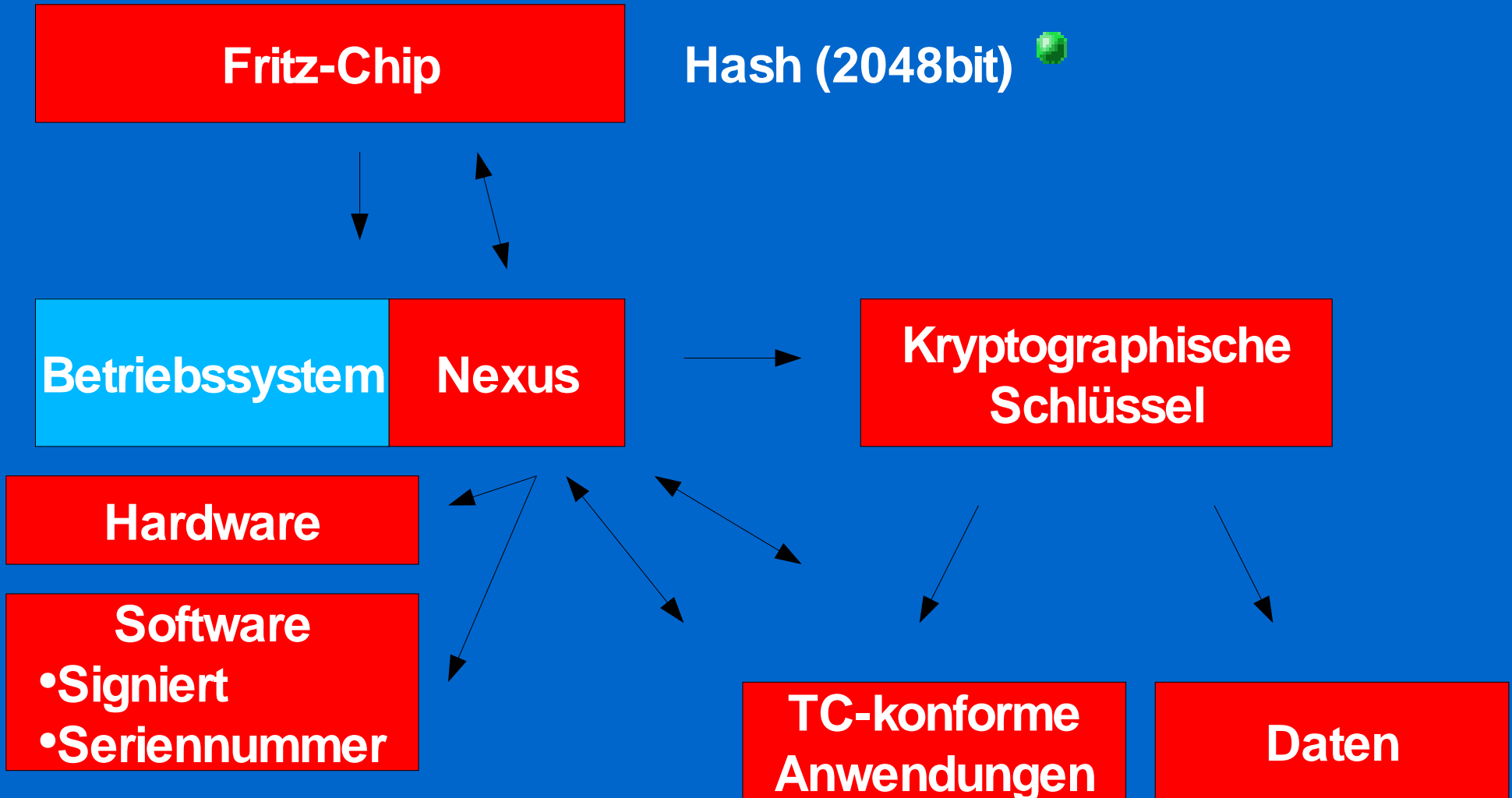
Hardware

Software

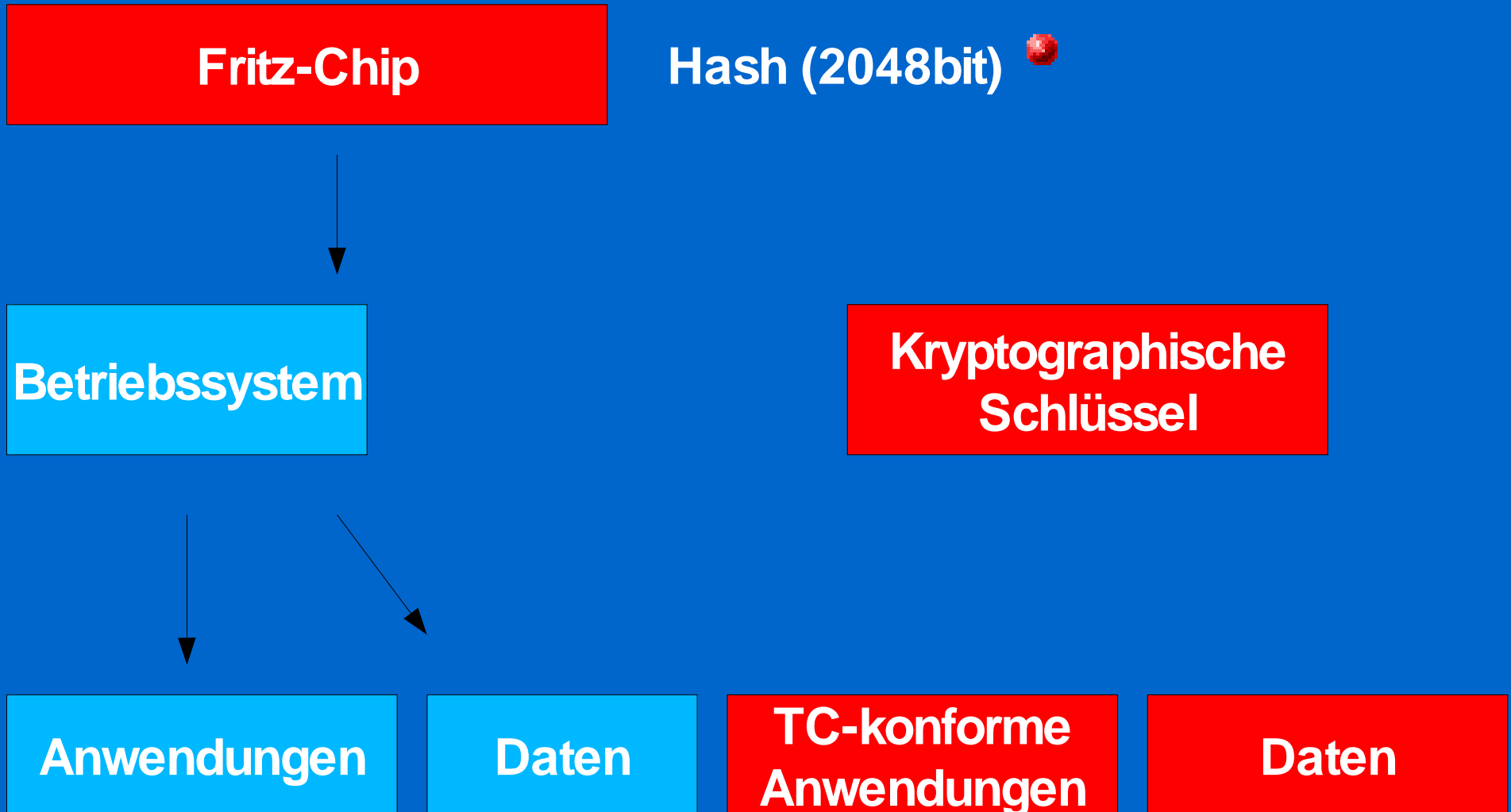
- Signiert
- Seriennummer

TC-konforme
Anwendungen

Daten



Wie funktioniert es?



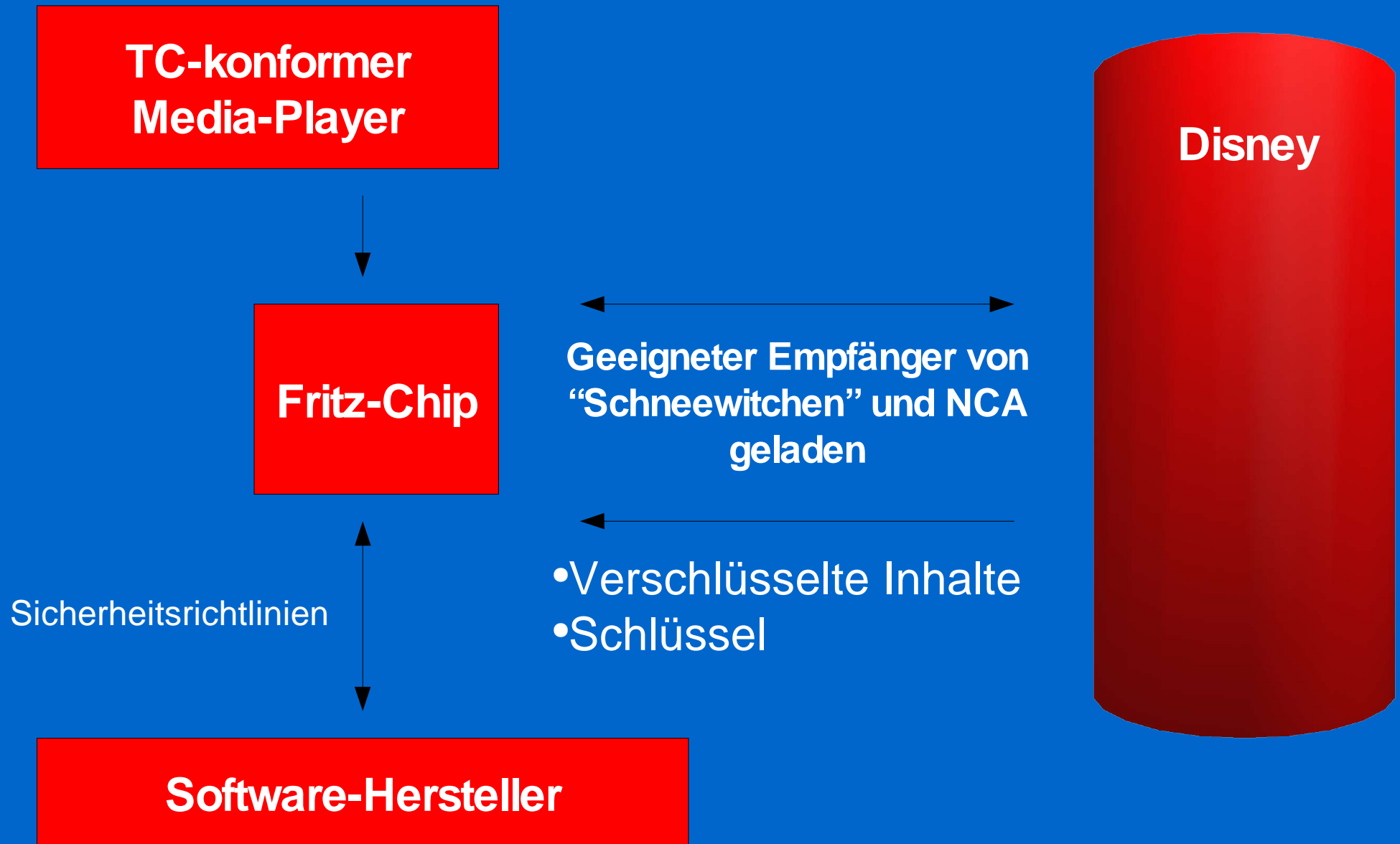
Wie funktioniert es?

Betriebssystem

Nexus

- Der Nexus arbeitet mit den abgesicherten Speicherbereichen der CPU zusammen.
- Stellt sicher das TC-Anwendungen Daten anderer TC-Anwendungen weder lesen noch verändern können.
 - “LaGrande Technologie” (LT) bei Intel CPUs
 - “TrustZone” bei ARM

Wie funktioniert es?



Wozu kann TC noch verwendet werden?

- Stärkere Zugangskontrolle zu vertraulichen Dokumenten
 - “Enterprise Rights Management” in Windows Server 2003
- Automatische Zerstörung von Dokumenten
 - Nach einigen peinlichen Enthüllungen interner Emails im Antitrust-Verfahren gegen Microsoft, führte Microsoft eine Richtlinie ein, derzufolge interne Mails nach 6 Monaten gelöscht werden müssen.
- TC kann ziemlich ausgefallene Kontrollen durchsetzen
- Zahlungssysteme (Micropayment)

Kann TC nicht geknackt werden?

- Abhören des unverschlüsselten Datenverkehr auf dem Bus zwischen CPU und Fritz-Chip (Phase I)
- Internen Datentransfer in der CPU (Phase II)
- Illegal durch:
 - DMCA
 - EU Copyright Richtlinie
 - Verordnung zur Durchsetzung
- Verbindung Kompatibilitätskontrolle <----> Copyrightkontrolle
 - Bei der Sony Playstation 2 beinhaltet der Authentifizierungschip gleichzeitig den Algorithmus zum Entschlüsseln von DVDs.

Wie kann TC missbraucht werden?

- Eine zentrale Löschung von raubkopierten Inhalten
- Traitor-Tracing
 - Der Besitzer wird strafrechtlich verfolgt
 - Alle Songs die über diesen PC wanderten werden geblacklisted
- TC-konforme PCs verweigern das Öffnen von Dokumenten die mit raubkopierten Versionen erstellt wurden.
- Ausstechen unliebsamer Mitbewerber
- Ökonomische Kriegsführung
- Politische Zensur

Kann man TC nicht einfach abschalten?

- **Kein Zugriff auf:**

- Daten
- Konto
- Software

- **TC-konforme Anwendungen werden schlechter oder gar nicht laufen.**

- **Die Anzahl der Anwendungen wird geringer sein.**

Die Auswirkungen

- Ich kann also keine MP3s mehr auf meinem Rechner hören?
 - Bereits vorhandene MP3s sollten für eine gewisse Zeit kein Problem sein.
 - Zustimmung von Anti-Raubkopiermaßnahmen seitens Microsoft (inc. dem löschen raubkopierter Inhalte)

Die Auswirkungen

- **Neue Geschäftsmodelle**

- **CDs zu einem Drittel des Preise die man nur 3 mal abspielen kann und bei Zahlung der restlichen 2 Drittel erhält man die kompletten Rechte**
- **Kopien digitaler Musik verleihen wobei die Originale auf der eigenen Festplatte gesperrt werden bis man die Kopien zurück bekommt.**

Die Auswirkungen

- **Wirtschaftliche Aspekte**

- **Tintenpatronen**
- **Handy-Akkus**
- **Speicherkarten bei PS2 und X-Box**
- **Zukünftig werden Entwickler ihre Formate TC-konform machen und den Zugang an Dritte vermieten.**
- **TC-konforme Anwendungen werden der Softwarefirma mehr Geld einbringen, da sie den Zugang zu den Schnittstellen für jeden Preis, den der Markt noch hergibt, vermieten kann.**

Die Auswirkungen

- **Wirtschaftliche Aspekte**

- Die Medienindustrie wird ihren Anteil durch die Verhinderung von Raubkopien machen
- Marktwerte von Intel, IBM und Microsoft werden steigen
- Stärkung der Position von Informationsinhabern- und Dienstleistern auf Kosten neuer Marktteilnehmer
- Regionale Effekte
 - Einbruch von Smartcard Verkäufe sobald in Phase II die Fritz-Funktionalität in die CPU integriert wird

Die Auswirkungen

- Politische Probleme

- Die Transparenz der Verarbeitung persönlicher Daten, die in der EU-Richtlinie zum persönlichen Datenschutz festgelegt ist
- Die nationale Souveränität, ob Copyright Regelungen von den Nationalparlamenten oder von Firmen in Redmond und Portland festgelegt werden
- Ob sich Leute mit dem Gedanken anfreunden können, dass ihr PC tatsächlich unter externer Kontrolle steht
- Kontrolle, deren sich Gerichte und Regierungsorgane ohne ihr Wissen bemächtigen können.

Die Auswirkungen

- **Autsch. Was noch?**
 - **TC wird die Gnu Public License (GPL) untergraben**
 - **IBM und HP haben anscheinend mit der Arbeit an TC erweiterten Versionen von GNU/Linux begonnen.**

Die Auswirkungen

- Wann wird es losgehen?
 - Spezifikationen wurden 2000 herausgegeben
 - IBM Thinkpad x30
 - Windows XP
 - X-Box
 - Windows Server 2003

Sonstiges

- Ist ein sicherer PC den keine tolle Sache?
- Warum spricht man vom “vertrauenswürdigen Computereinsatz”?

Vielen Dank

Weitere Informationen unter:
<http://www.againsttcpa.com>

Fragen, Anregungen an:
NachtKind@io.ccc.de

Spenden an:
Chaos Computer Club e.V.
Postbank Hamburg
Konto-Nummer 1765 3201