DRM und Trusted Computing – Herr der eigenen Hardware?

MASTERARBEIT

Im Studiengang Medienautor (Master)

Fakultät Electronic Media

Fachhochschule Stuttgart – Hochschule der Medien

Erstprüfer:	Prof. Walter Kriha
Zweitprüfer:	Prof. Dr. Roland Schmitz

Vorgelegt von:

Peter Dietrich
Lange Anwanden 42
71065 Sindelfingen
Matrikel-Nr. 15196

Sindelfingen, 31. Dezember 2006

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Masterarbeit selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht.

_____ _____

Ort, Datum Unterschrift

Kurzfassung

Diese Masterarbeit analysiert die beiden oft miteinander in Verbindung gebrachten Themen Trusted Computing und Digital Rights Management. Sie erläutert die Grundlagen von Trusted Computing, fasst die Ziele der Arbeitsgruppen der TCG zusammen und gibt einen Überblick über aktuelle Anwendungen. Zum Thema Digital Rights Managements betrachtet sie die Grundlagen und nennt die Punkte, die am häufigsten an DRM und Trusted Computing kritisiert werden. Aktuelle Ereignisse zeigen die Tendenzen auf, die momentan die Entwicklung von DRM und Trusted Computing beherrschen. Die Arbeit kommt zu dem Ergebnis, dass zukünftige Trusted Systems technisch in der Lage sind und aus Sicht der Hersteller sein sollen, Teile des Systems der Kontrolle durch den User zu entziehen und somit die Durchsetzung von Einschränkungen unterstützen können

Abstract

This master thesis analyses the both topics Trused Computing and Digital Rights Management that are often related to each other. It illustrates the basics of Trusted Computing, summarizes the goals of the TCG's workgroups and provides an overview of current applications. It examines the basics of Digital Rights Management and reflects the issues that are most commonly criticised. Present events show the trends that currently dominate the development of DRM and Trusted Computing. The master thesis concludes that future Trusted Systems will and – from a manufacturer's view – should technically be able to revoke the user's control of parts of the system and thus can support the enforcement of restrictions.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AIK	Attestation Identity Keys
DMCA	Digital Millennium Copyright Act
DRM	Digital Rights Management
EK	Endorsement Key
EMSCB	European Multilaterally Secure Computing Base
HMAC	Hashing for Message Authentication Calculator
MLTM	Mobile Local-Owner Trusted Module
MRTM	Mobile Remote-Owner Trusted Module
MTM	Mobile Trusted Module
NGSCB	Next Generation Secure Computing Base
PCR	Platform Configuration Register
SRK	Storage Root Key
TBB	Trusted Building Block
TC	Trusted Computing
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TCS	TSS Core Service
TDDL	TSS Device Driver Library
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TSP	TSS Service Providers
TSS	Trusted Software Stack
WSDL	Web Service Description Language

Vorwort

Hinweise zu den Angaben von Quellen – Deep Links

Die meisten Quellenangaben der Arbeit sind URLs von Webseiten, auf denen die verwendeten Informationen zu finden sind. Sofern es sich um Deep Links handelt (also auf eine Unterseite der Internetpräsenz verwiesen wird), sind diese mit Keywords versehen. Über diese Keywords sollte die Quelle unter Verwendung einer Suchmaschine (hauptsächlich wurde bei der Erstellung der Arbeit google.de verwendet) wieder gefunden werden. Zusätzlich sollte die Quelle auf diesem Weg auch dann wieder gefunden werden, wenn der Anbieter die Struktur seiner Webpräsenz ändert. Auf die Angabe eines Zugriffsdatums wurde in diesem Fall verzichtet.

Hinweise zu den Angaben von Quellen – Wikipedia

Bei Quellenangaben, die auf die freie Enzyklopädie wikipedia.de bzw. wikipedia.com verweisen, wird das Datum der Version angegeben, auf die sich ein Zitat oder eine Abbildung bezieht.

1 Einleitung

DRM (Digital Rights Management), der Schutz von digitalem Inhalt sowie Trusted Computing, also die Schaffung einer vertrauenswürdigen Plattform für sicheres Computing, werden seit einigen Jahren unweigerlich miteinander in Verbindung gebracht. Obwohl heutige DRM System eigenständig funktionieren und Trusted Computing ganz allgemein den Anspruch erhebt, Rechner von heute sicherer und vertrauenswürdiger zu machen, so wird das Zusammenspiel der beiden Technologien in vielen Szenarien als äußerst bedenklich bezeichnet.

Kritikern sehen in der Kombination Möglichkeiten der Überwachung und Entmündigung der User: Angestoßen durch die Interessen der Musik- und Filmindustrie, mit dem Ziel, die illegale Vervielfältigung bzw. Nutzung von digitalem Inhalt nicht nur rechtlich, sondern auch technisch, einzugrenzen.

Während einer Diskussion in einer Vorlesung über dieses Thema kam für mich die Frage auf, ob ich in wenigen Jahren noch Herr meiner eigenen Hardware bin, oder ob sich gar irgendwann meine Grafikkarte – oder spätestens mein Bildschirm – weigern würde, einen Film abzuspielen, der bestimmten Vorgaben nicht entspricht?

Ziel dieser Arbeit ist, Trusted Computing und DRM aus aktueller Sicht zu beleuchten. Da kaum objektive Zusammenfassungen der Arbeit der TCG (Trusted Computing Group) zu existieren scheinen, soll die Arbeit einen objektiven Überblick über die tatsächlichen Spezifikationen bieten. Diese Erkenntnisse sollen dazu dienen, einschätzen zu können, welche Ziele von Entwicklungs- und Herstellerseite verfolgt werden, wie die Systeme heute eingesetzt werden und wie sich diese Verwendungen weiterentwickeln könnten. Wie ist die heutige Stellung von DRM und TC und welche Anstrengungen werden weiterhin unternommen, diese Technologien miteinander zu verknüpfen? Und in wie weit wird auf die Punkte der Kritiker eingegangen?

2 Trusted Computing

2.1 Begriffsdefinition und Historie

2.1.1 Trusted Computing und die TCPA

Der Begriff „Trusted Computing“ wurde geprägt durch das 1999 gegründete Konsortium der „Trusted Computing Platform Alliance“ (TCPA). Das Ziel des Konsortiums war, eine vertrauenswürdige Plattform für Computersysteme zu schaffen, auf der Hardware und Software in einem gesicherten Zustand betrieben werden können. Dieser sichere und vertrauenswürdige Modus soll bestimmten Sicherheitsanforderungen gerecht werden und eine Überprüfbarkeit bzw. Integrität des Systemzustands ermöglichen.

Das Konsortium bestand bei der Gründung aus den ‚Größen' der Computerindustrie Microsoft, Hewlett-Packard, IBM und Compaq. Weitere Software- und Hardwarehersteller schlossen sich an und so wurden ca. 200 Unternehmen Mitglieder der TCPA. Der basisdemokratische Aufbau des Konsortiums sowie die Tatsache, dass jedes Mitglied ein Veto-Recht besaß, schränkten die TCPA allerdings in ihrem Handlungsspielraum ein.

2.1.2 Trusted Computing Group

Offiziell wurde aufgrund der oben genannten Probleme die TCPA im April 2003 von der „Trusted Computing Group“ (TCG), gegründet von AMD, Hewlett-Packard, IBM, Intel und Microsoft, abgelöst. Die Organisation bekam einen Vorstand und einen festeren Rahmen. Das Veto-Recht aller Mitglieder wurde abgeschafft, für Beschlüsse reichte seither eine 2/3-Mehrheit. Es wurden verschiedene Stufen der Mitgliedschaft[1] eingeführt: Promoter, Contributor und Adopter. Diese unterscheiden sich in den Mitspracherechten, Einflussmöglichkeiten und nicht zuletzt den Mitgliedsbeiträgen, die an die TCG gezahlt werden (von $1.000, ursprünglich $7500, bis $50.000 pro Jahr).

[1] https://www.trustedcomputinggroup.org/about/members/ - Aktuelle Liste der Mitglieder der TCG
Keywords: tcg members

Alle Mitglieder der TCPA und weitere Unternehmen wurden eingeladen, der TCG beizutreten und gemeinsam die bisherigen Entwicklungen (Spezifikationen) der TCPA zu übernehmen und weiterzuentwickeln.

Das Ziel der TCG wurde neu definiert: Offene Standards, Spezifikationen für PCs, Server, Laptops, PDAs, Mobiltelefone im Bereich der Hardware und auch Softwareschnittstellen. Alle Überlegungen basieren weiterhin auf einer „root of trust", einem Chip, der – in allen Geräten enthalten – für die Basis der sicheren Kommunikation sorgen soll.

Heute unterteilt sich die Arbeit der TCG in mehrere Workgroups, deren Aufgaben in die verschiedenen Anwendungsgebiete aufgeteilt sind. So werden die Gruppen in die Bereiche

- Infrastructure
- Mobile
- PC Client
- Server
- Software Stack
- Storage
- Trusted Network Connect (Untergruppe der „Infrastructure"
- Trusted Platform Module (TPM)

aufgeteilt. Hierbei stellt das Trusted Platform Module (TPM) einen kleinen Chip dar, der als Hardware auf den Geräten verbaut wird, die zu einer Trusted Computing Umgebung gehören. „Software Stack" bezeichnet die Spezifikationen, die von Seiten der Softwareentwicklung benutzt werden, um mit dem TPM in Kontakt zu treten. Die anderen Gruppen beschäftigen sich hauptsächlich mit den Einsatzgebieten in entsprechenden Endgeräten bzw. sicherer Netzwerkkommunikation (z. B. VPN oder Authentifizierung).

Eine ‚fertige' Spezifikation gibt es noch nicht. Die Gruppen arbeiten ständig an den Erweiterungen. Momentan (Dezember 2006) ist die Version TCG 1.2 aktuell und

wird von den meisten Hardware- und Softwareherstellern verwendet und integriert. Teilweise wird noch eine Abwärtskompatibilität zu der vorherigen Spezifikation TCG 1.1b sichergestellt.

2.2 Entwicklungen und Spezifiaktionen der TCG

2.2.1 TPM – Trusted Platform Module

Grundbaustein der Geräte in einer Trusted Computing Umgebung ist das TPM, das Trusted Platform Modul. Das TPM ist ein eigenständiger Chip, der direkter Teil des Prozessors bzw. Bestandteil der Hauptplatine ist. Er wird in seiner Funktionsweise oftmals mit einer ‚aufgelöteten Smartcard' verglichen, ist aber im Gegensatz zu dieser fest an das System und nicht an den Benutzer gebunden.

Der Chip wurde in den ersten Entwicklungstagen der TCPA von Kritikern auch mit dem Spitznamen ‚Fritz Chip' bezeichnet. Dies geht auf den ehemaligen US-Senator Fritz Hollings zurück, der sich für den Schutz von geistigem Eigentum stark machte und ein Gesetz unterstütze, das einen derartigen Chip in jedem Gerät forderte. Diese Bezeichnung ist mittlerweile weitgehend verschwunden. Heute wird meist der korrekte Name TPM oder auch ‚TCG Chip' benutzt, in älteren Beschreibungen wird vereinzelt noch die Bezeichnung ‚TCPA Chip' verwendet.

Das TPM ist so ausgelegt, dass es beim Start eines Systems aktiviert oder deaktiviert werden kann (z. B. über BIOS Einstellungen), somit das System auf Wunsch des Eigentümers mit oder ohne TCG-Unterstützung gestartet werden kann. Die Deaktivierung führt allerdings dazu, dass Komponenten, die TPM-Unterstützung voraussetzen, nicht in vollem Umfang oder gar nicht zur Verfügung stehen können.

Der Chip birgt Speichereinheiten, funktionale Einheiten und mehrere integrierte Schlüssel, die – teils fest, teils variabel – für die verschiedensten Anwendungszwecke benutzt werden können.

2.2.1.1 Aufbau

Die folgende Darstellung zeigt den schematischen Aufbau des Trusted Platform Modules.

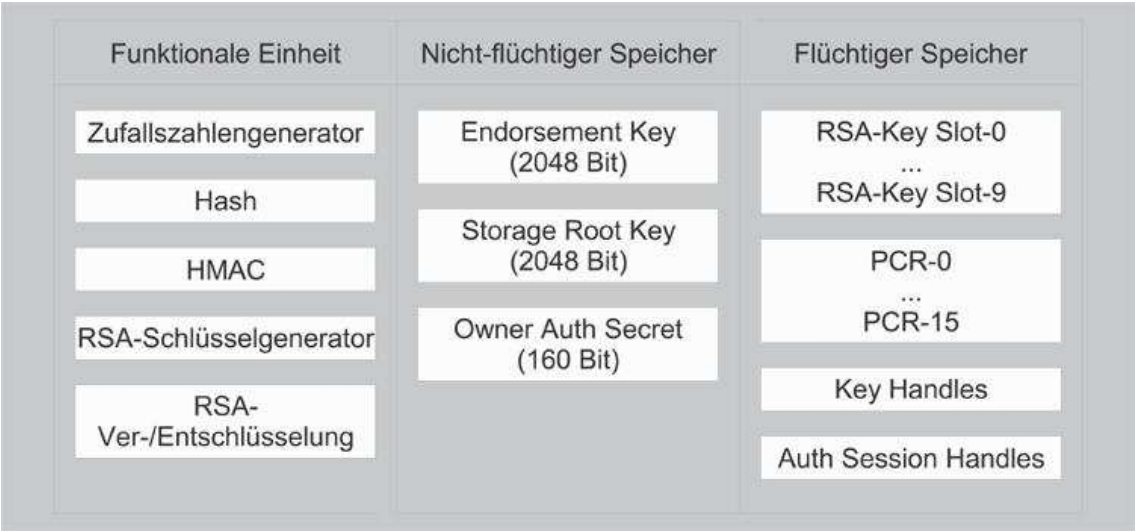

Abbildung 1: Schematischer Aufbaus des TPMs

Quelle: http://www.linux-magazin.de/Artikel/ausgabe/2006/04/tcpa/tcpa.html (2006-12-26)

2.2.1.2 Funktionale Einheiten

Zufallsgenerator

Das TPM enthält einen Zufallsgenerator, der zuverlässige Zufallszahlen liefern soll. Die Spezifikation schlägt vor, mehrere physikalische Werte des Systems wie z. B. auch Temperaturinformationen über das System bei der Generierung von Zufallszahlen zu integrieren, um unvorhersehbare Zahlen liefern zu können. Zufallszahlen spielen gerade in der Kryptografie (z. B. bei der Generierung von Schlüsselpaaren) eine wichtige Rolle. Die erzeugten Zufallszahlen werden sowohl intern vom TPM benutzt, können aber auch anderen Applikationen zur Verfügung gestellt werden.

Ver- und Entschlüsselungseinheiten

Um das System von Verschlüsselungsvorgängen zu entlasten und diese auch sicher ablaufen zu lassen, sieht das TPM mehrere funktionale Einheiten vor, die Hash-Bildungen (SHA-1), die Generierung von RSA-Schlüsseln und RSA-Ver- und Entschlüsselungen direkt auf dem Chip durchführen können. Das HMAC („Hashing for Message Authentication Calculator“) signiert Daten speziell für den Email-Verkehr.

2.2.1.3 Schlüssel

Endorsement Key (EK)

Der „Endorsement Key“ ist ein das TPM eindeutig identifizierendes Schlüsselpaar mit 2048 Bit Länge, das auf dem RSA-Verfahren beruht. Dieser Schlüssel wurde in der Spezifikation im Laufe der Entwicklungen der TCG auf Druck von Kritikern von einem unveränderbaren zu einem überschreibbaren Key verändert. Da er benutzt werden kann, um ein TPM – somit ein Endgerät und damit auch einen Benutzer – zu identifizieren, wurde festgelegt, dass er auch wieder überschrieben und durch einen neu generierten Schlüssel ersetzt werden kann. Somit ist z. B. eine Identifikation eines vom Hersteller ausgelieferten TPMs und ein Zuordnung zum Käufer im Nachhinein nicht mehr möglich.

Der EK könnte verwendet werden, um die Existenz eines TPM auf einem Gerät und auch die Vertrauenswürdigkeit eines Gerätes zu bestätigen. Allerdings würde dabei jedes Mal der gleiche öffentliche Schlüssel des TPM verwendet und eine Zuordnung verschiedener Anfragen, Seitenaufrufen, oder Verbindungen mit einem Dienst könnten einem bestimmten TPM zugeordnet werden. Um dies zu verhindern, wurden „Attestation Identity Keys“ eingeführt, die dieses Problem der Privatsphäre umgehen.

Attestation Identity Keys (AIK)

Um für Identifizierungsvorgänge nicht den EK verwenden zu müssen, kann der User – ausgehend von seinem gültigen EK – weitere Pseudonyme generieren, die für solche Zwecke eingesetzt werden können. Diese Schlüssel, welche für die Beglaubigung (siehe 2.2.2.3 Beglaubigung (Remote Attestation)) verwendet werden, können in beliebiger Anzahl erzeugt werden und sind auch nur für einen Vorgang gültig (‚Wegwerfschlüssel’). Sie werden für den Zeitraum der Verwendung in einem der flüchtigen RSA-Key Slots zwischengespeichert.

Storage Root Key (SRK)

Das TPM ist in der Lage, Schlüssel aller Art sicher zu verwahren. Dazu gehören z. B. Schlüssel anderer kryptographischer Systeme oder auch Passwörter. Dieser werden im TPM wiederum selbst verschlüsselt abgelegt. Dieser Schlüssel-Safe wird mit dem Storage Root Key, also dem ‚Wurzelschlüssel’ aller abgelegten Schlüssel verschlüsselt.

Dieser wird beim Übernehmen der Hardware durch den Benutzer erzeugt – und sollte vom Anwender auch nicht vergessen werden, da sonst der Zugriff auf die damit verschlüsselten Daten nicht mehr gewährt werden kann.

Owner Authorization Secret

Dies bezeichnet einen 160 Bit Schlüssel, den der Benutzer selbst wählt und der verwendet wird, um bestimmte sensitive Vorgänge vom Benutzer direkt bestätigen zu lassen.

2.2.1.4 Speicherbereiche

RSA-Key Slots

Die Key Slots werden verwendet um AIKs zu speichern bzw. bei RSA-Operationen benutzt.

PCR („Platform Configuration Register")

Diese beinhalten 160 Bit Hash-Werte, die Aufschluss über das System geben. Dazu gehören z. B. Informationen über das BIOS, Master Boot Record, Bootloader, bestimmte System- oder Kerneldateien sowie Hardware. Wenn an der Konfiguration des Systems keine Änderungen vorgenommen wurden, beinhalten diese Register bei jedem Bootvorgang die gleichen Daten und somit kann das Booten eines Systems in einen genau bestimmten bzw. gesicherten Zustand überwacht werden.

Key/Authorization Session Handles

In den Key Handles wird verwaltet, welcher Key in den Speicherblöcken zu welchem Bearbeitungsschritt gehört, während die Session Handles bei mehreren ablaufenden Autorisationen den Status überwachen.

2.2.1.5 Weiterführende Quellen zum Thema

http://www.linux-magazin.de/Artikel/ausgabe/2006/04/tcpa/tcpa.html

https://www.trustedcomputinggroup.org/groups/tpm/

Keywords: tcpa tcg tpm endorsement

2.2.2 Funktionen

2.2.2.1 Versiegelung (Sealing)

Grundgedanke dieser Funktion ist, Daten beliebiger Art an ein System bzw. eine Systemkonfiguration (Hardware und Software) zu binden und somit nur auf diesem System lesbar zu machen. Dies geschieht über einen Hash, der die momentane Konfiguration abbildet. Berücksichtigt werden dabei auch die Inhalte der PCR des TPMs, die Informationen über die Konfiguration von Systemkomponenten liefern. Daten können somit nur wieder gelesen werden, wenn der vorher definierte Systemzustand (also die entsprechende Konfiguration aus Hardware und Treibern) wiederhergestellt wurde, d.h. in einen ‚vertrauenswürdigen Zustand' gebootet wurde.

2.2.2.2 Auslagerung (Binding)

Grundgedanke hier ist, Daten verschlüsselt außerhalb des TPMs auszulagern, aber mit den Schlüsseln des TPMs zu sichern. Somit könnten Daten aller Art auf der Festplatte oder anderen Datenträgern abgelegt werden, aber nur vom Benutzer, der Zugriff auf den SRK des TPMs hat, wiederhergestellt werden.

2.2.2.3 Beglaubigung (Remote Attestation)

Bei diesem Verfahren soll gewährleistet werden, dass sich das System mit dem TPM gegenüber einem Dienstanbieter als vertrauenswürdig und mit einem gültigen TPM ausgestattet ausweisen kann.

Die erste Spezifikation der TCG sah vor, dass der öffentliche Teil des EK von einer vertrauenswürdigen dritten Stelle, einer Privacy Certification Authority überprüft und signiert wird. Dabei ist ausschlaggebend, dass das TPM mit seinem Endorsement Key nicht als ungültig eingestuft („blacklisted") wurde.

In einer Änderung der Spezifikation wurde der EK durch die bereits oben beschriebenen AIKs ersetzt, um zwar die Vertrauenswürdigkeit des TPMs bestätigen zu können, aber keine direkte Identifizierung des TPMs durch die Bekanntgabe des EK an den Dienstanbieter zuzulassen.

Da diese Lösung den Nachteil hat, dass an die Certification Authority hohe Verfügbarkeitsanforderungen gestellt werden (und der Anspruch an die Sicherheit der Privatsphäre nicht gewährleistet werden kann, wenn Privacy CA und Dienstanbieter kooperieren), wurde in einer weiteren Version die Direct Anonymous Attestation[2] als zweite Möglichkeit der Beglaubigung vorgesehen.

Dabei beweist das TPM in mehreren Schritten, dass es im Besitz eines von einer CA signierten AIK ist und den dazugehörigen Private Key kennt, ohne dass das TPM die Details bekannt geben muss. Somit ist für den Dienstanbieter gewährleistet, dass er Kontakt zu einem vertrauenswürdigen TPM hat. Der Benutzer bzw. das TPM kann aber nicht bei jeder Transaktion identifiziert oder rückverfolgt werden.

2.2.2.4 Zufallsgenerator

Der integrierte Zufallsgenerator soll nicht nur für die interne Generierung von Schlüsseln dienen, sondern auch anderen Applikationen zur Verfügung gestellt werden können.

2.2.3 TSS – Trusted Software Stack

Der TSS „Trusted Software Stack" ist die Schnittstelle bzw. API, in der definiert wird, wie von Seiten einer Application auf die Funktionen des TPM zugegriffen werden soll bzw. wie von Herstellerseite der Aufbau implementiert werden soll. Die Spezifikation der TCG ist herstellerneutral und soll unabhängig von der verwendeten Hardware oder dem Betriebssystem auf jedem System verwendet werden können.

2.2.3.1 Aufbau des TSS

Der Software Stack wird in mehrere Schichten unterteilt:

---

[2] http://www.zurich.ibm.com/security/daa/ - Informationen zur Entwicklung der DAA
Keywords: direct anonymous attestation
und
TCG Software Stack Specification Version 1.2, Level 1, 11. Jan 2006, Seite 402 ff (Detaillierter Ablauf)
Keywords: tcg tss specification

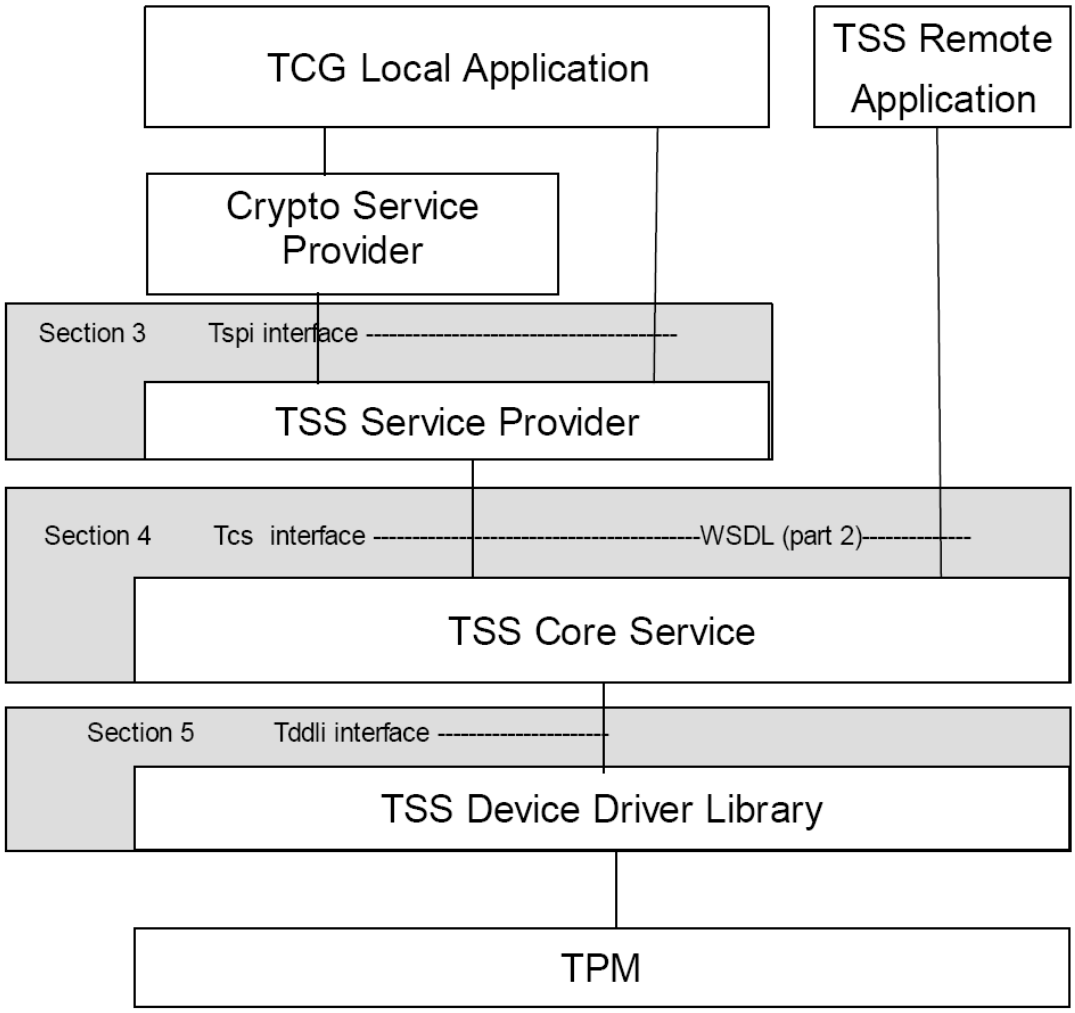

Abbildung 2: TSS Block Diagramm

Quelle : TCG Software Stack Specification Version 1.2, Level 1, 11. Jan 2006, Seite 30

TSS Device Driver Library (TDDL)

Für den direkten Zugriff auf das TPM sieht die TSS eine Device Driver Library vor, die vom Hersteller des TPM implementiert und zur Verfügung gestellt werden muss. Dieser Treiber hat direkten Zugriff auf das TPM und regelt die Ansteuerung des Moduls. Da dies direkten Zugriff auf die Hardware voraussetzt, muss der Treiber aus der Sicht des Betriebssystems im Kernel Modus laufen.

Der Zugriff auf den Treiber wiederum ist in der Schnittstellenspezifikation des TDDL Interface (Tddli) festgelegt. Dies stellt sicher, dass unterschiedliche Versionen oder Implementierungen der darüber liegenden Schicht gleichermaßen auf die TDDL zugreifen können.

TSS Core Service (TCS)

Der TSS Core Service ist systemseitig für die Verwaltung der Zugriffe auf das TPM bzw. den Treiber zuständig. Da kein direkter Zugriff auf die Hardware notwendig ist, läuft der Core Service im User Mode des Betriebssytems als einmaliger Systemservice und verwaltet die Zugriffe mehrerer Applikationen. Der direkte Zugriff einer Applikation auf das TPM bzw. den Treiber ist nicht zulässig, sondern muss durch den TCS erfolgen. Komplexe Operationen werden vom TCS nicht angeboten, lediglich einfache Funktionen werden über das TCS Interface (Tcsi) den oberen Schichten bereitgestellt. Komplexe Prozesse mit mehreren Teilschritten müssen von den oberen Schichten selbst verwaltet werden.

TSS Service Providers (TSP)

TSS Service Providers sollen die Verwendung des TPM so weit vereinfachen, dass sie komplexe Vorgänge als objektorientiert zusammengefasste Funktionalitäten anbieten und den Applikationen somit standardisierte Prozesse anbieten. Die Schlüsselverwaltung oder Byte Stream Erzeugung soll somit vom TSP verwaltet werden, was die Entwicklung von Applikationen vereinfachen soll. Dabei werden u. U. auch Teile der Vorgänge nicht zwangsläufig direkt im TPM sondern im Software Stack abgearbeitet. Dafür sind mehrere Objektklassen in der Spezifikation vorgesehen, die Aufgaben wie Hashing, Datenverschlüsselung (für Sealing und Binding) oder die Bereitstellung eines definierten Status der PCR übernehmen.
TSPs sind ‚pro Applikation' gedacht, d. h. es wird nicht wie der TCS ein globaler Service laufen, sondern jede Applikation kann nach eigenen Bedürfnissen einen TSP benutzen.

Remote Procedure Calls

Die Spezifikation sieht vor, dass durch den TSS sichere Verbindungen zwischen TPMs erstellt und Aufrufe von einer Seite zur anderen gestartet werden können. Auf diese Weise können Systeme ihren TCS anderen Systemen zur Verfügung stellen, um über SOAP Services anzubieten.
Die spezifizierten Funktionen sind über die „Web Service Description Language" (WSDL) geregelt.

2.2.3.2 Weiterführende Quellen zum Thema

Die Abbildung 3: TSS Architektur Diagramm zeigt einen detaillierten Aufbau des TSS mit weiteren Funktionen, die ein vollständiger Software Stack anbieten kann bzw. soll. Details hierzu finden sich in der 742-seitigen Spezifikation der TCG zum Thema TSS (TCG Software Stack Specification Version 1.2, Level 1, 11. Jan 2006), zu finden unter https://www.trustedcomputinggroup.org/groups/software/

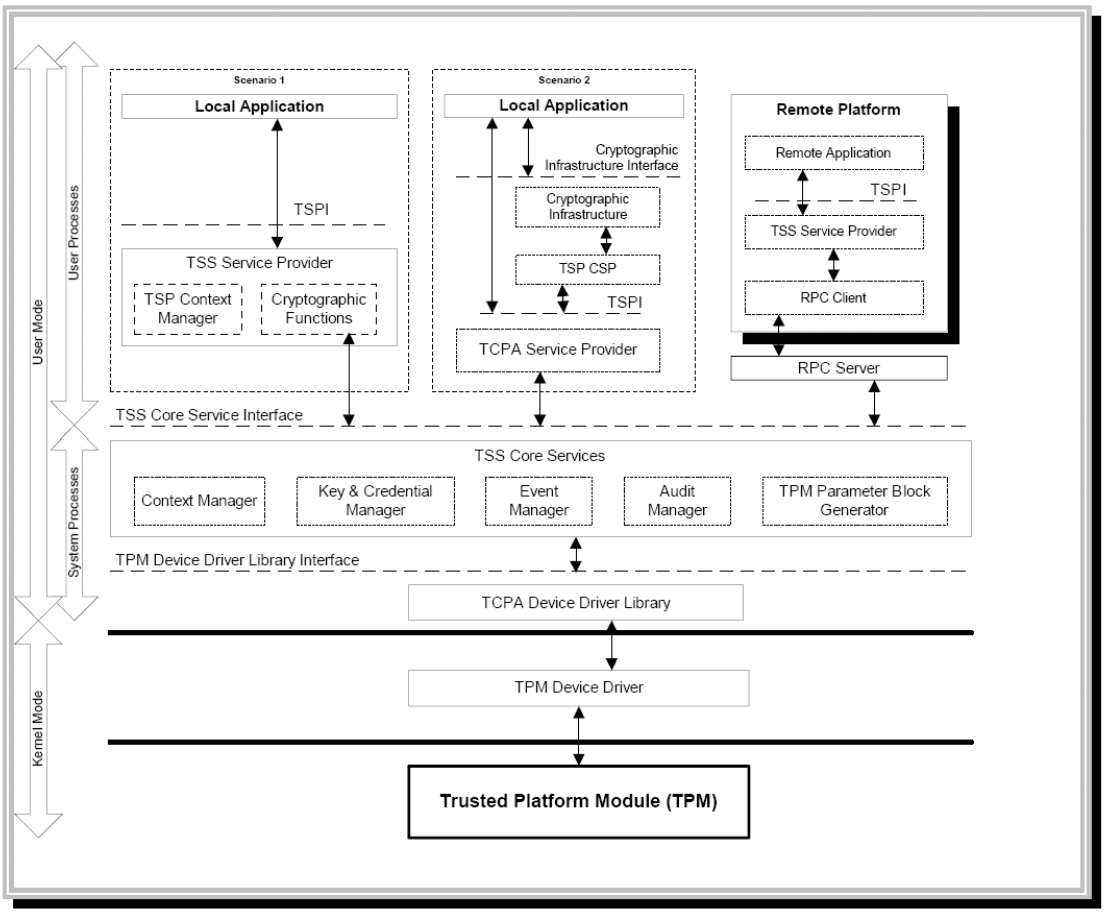

Abbildung 3: TSS Architektur Diagramm

Quelle : TCG Software Stack Specification Version 1.2, Level 1, 11. Jan 2006, Seite 39

2.3 Einsatzgebiete von Trusted Computing

Die Trusted Computing Group hat sich zum Ziel gesetzt, Spezifikationen zu erstellen, die für alle Bereiche des heutigen „Computings“ gültig sind. In den folgenden Kapiteln sollen Anwendungsbereiche dargestellt werden, die zukünftig oder auch heute schon sowohl beispielhaft als auch in Produktiv-Umgebungen die Spezifikationen der TCG integrieren.

2.3.1 Vorgeschlagene Einsatzszenarien von Seiten der TCG

In ihrem Dokument „TCG Architecture Overview“ zeigt die TCG vier exemplarische Möglichkeiten auf, bei denen Trusted Platforms helfen sollen. Zu den vorgeschlagenen Verwendungszwecken gehören:

Risk Management

Beim Verlust eines Systems sind die Daten nicht nur verloren, sondern können auch in die falschen Hände geraten. Die Verbesserung bei der Verwendung von TPMs zielt darauf ab, dass Schlüssel und Passwörter nicht zugänglich sind, wenn sie sicher im TPM abgelegt bzw., mit Hilfe des TPMs verschlüsselt werden.

Asset Management

Da der „Owner“ eines TPMs nicht zwangsläufig der Benutzer des Systems sein muss, kann die administrative Kontrolle über Systeme bei einem „Asset Manager“ eines Unternehmens bleiben. Somit sind Systeme jederzeit eindeutig identifizierbar und können auch nach einer Neuinstallation erkannt werden.

E-Commerce

Der wohl meist diskutierte Einsatz des TPM ist der für den E-Commerce bzw. Transaktionen zwischen Nutzer und einem Dienstanbieter. Das Beispiel der TCG sieht zwei Möglichkeiten vor: Einerseits soll der Benutzer durch Wiederherstellung bestimmter Einstellungen Vorteile davon haben, dass ihn ein Dienstanbieter als treuen Kunden identifizieren kann.

Andererseits habe der Anbieter die Möglichkeit, Informationen über die Konfiguration der Plattform zu erhalten und auf diese Weise sicherzustellen, dass der Datenaustausch im gleichen Kontext wie vorherige Transaktionen ablaufen wird. Damit sei beiden Parteien das Vertrauen auf eine sichere Transaktion gewährt.

Security Monitoring and Emergency Response

Die Werte, die in den PCR abgelegt sind, erlauben Aufschluss über den Zustand einzelner Systeme und deren Konfiguration. So sind Administratoren in der Lage, diese Werte z. B. über einen Prozess, der diese Daten zentral weiterleitet, auszuwerten und gefährdete System zu identifizieren oder auch unerwünschte Änderungen am System (wie z. B. durch Virenbefall) zu erkennen.

2.3.2 Arbeitsgruppen der TCG

Die einzelnen Gruppen der TCG sind bestrebt, für verschiedenste Einsatzgebiete Erweiterungen der existierenden Mechanismen zu beschreiben, die die Sicherheit in den Systemen und deren Kommunikation erhöhen. (Die Arbeit der beiden Arbeitsgruppen „TPM“ und „TSS“ sind hier nicht noch einmal aufgeführt, siehe dazu 2.2.1 TPM – Trusted Platform Module sowie 2.2.3 TSS – Trusted Software Stack.)

2.3.2.1 Infrastructure Work Group

Die Arbeitsgruppe „Infrastructure“ beschäftigt sich mit zwei verschiedenen Aspekten der Infrastruktur. Zum einen mit der „Inter-Platform“ Infrastruktur, also der Art, wie zwei verschiedene unabhängige Plattformen miteinander kommunizieren, sowie der „Intra-Platform“ Infrastruktur, also dem Zusammenspiel eines TPM mit anderen Geräten in einem System.

Zu den Aufgaben der IWG gehört unter anderem auch, den „Platform Lifecycle“ zu bedenken. Dies beinhaltet, all die Mechanismen zu erarbeiten, die notwendig sind, um ein vom Hersteller vorgefertigtes TPM bzw. eine Plattform als Besitzer zu übernehmen, zu benutzen, und auch wieder abzugeben oder zu verkaufen, ohne dabei nachvollziehbar Spuren zu hinterlassen oder seine Identität weiterzugeben. All die dabei notwendigen Schritte, die von Herstellerseite und Benutzerseite notwendig sind und beachtet werden müssen, werden von der IWG beschrieben.

Ein weiteres Ziel der Arbeitsgruppe ist, alle notwendigen Schritte zu erarbeiten, die einem Nutzer die Migration seiner ‚Identität’ von einem existierenden auf ein anderes Gerät ermöglichen, ohne dass er auf dem vorherigen Gerät Spuren hinterlässt.

Zum Teil der „Inter-Platform“ Kommunikation gehören auch die Mechanismen, mit denen ein Client mit seiner Umgebung, darunter auch den Zertifizierungsstellen, kommuniziert und wie die einzelnen Schlüssel und Zertifikate präsentiert und ausgetauscht werden. Dazu gehört auch SKAE (Subject Key Attestation Evidence) mit dessen Hilfe ein Client beweisen kann, dass er der Besitzer eines privaten Schlüssels ist, der zu einem Zertifikat gehört.

2.3.2.2 Mobile Phone Work Group

Diese Arbeitsgruppe hat sich zum Ziel gesetzt, die Möglichkeiten der Gedanken des TPMs auf die mobile Welt der Mobiltelefone (und auf Smartphones) auszuweiten. Dabei soll allerdings nicht genau die Spezifikation des TPMs benutzt werden, sondern erweitert und an die Bedürfnisse für den mobilen Einsatz angepasst werden. So wird das TPM in der Spezifikation durch unter Umständen mehrere MTMs, (Mobile Trusted Modules) ersetzt. Diese MTMs werden in zwei grundsätzliche Typen unterschieden, MLTMs (Mobile Local-Owner Trusted Modules) und MRTMs (Mobile Remote-Owner Trusted Modules). Die Idee dabei ist, dass nicht nur der Benutzer, sondern auch der Mobilfunkanbieter oder der Hersteller des Endgerätes Möglichkeiten des kontrollierten und sicheren Zugriffs auf das Endgerät haben. Mehrere sog. „Stakeholder" (also Interessenten) sollen somit ihre individuellen Interessen am Endgerät kontrollieren und schützen können. Provider sollen damit die Möglichkeit haben, Voreinstellungen des Telefons anzupassen.

Das MTM soll Schlüssel und Daten schützen, auf die nur von Berechtigten zugegriffen werden kann. Dies kann auch dadurch erlangt werden, dass mehrere verschiedene Umgebungen in dem Endgerät gebootet werden, auf die nur der Besitzer zugreifen kann.

2.3.2.3 PC Client

Mit Überlegungen zur Integration der Grundgedanken eines TPMs in die heutigen Computersysteme auf Client-Seite beschäftigt sich diese Arbeitsgruppe. Die Absicherung eines Bootvorgangs in einen genau festgelegten Zustand und die damit verbundenen Maßnahmen werden hier spezifiziert.

Sozusagen ‚ab dem Einschalten' wird beschrieben, welche Einheiten bei diesem sicheren Booten zusammenarbeiten müssen. Dies beginnt bei einem sicheren BIOS in Form einer unveränderlichen „Wurzel des Vertrauens" (Core Root of Trust for Measurement – CRTM), die von Anfang an alle Vorgänge und darauf aufbauende Prozesse überwacht und sichert. Diese sichere BIOS wird z. B. vom Hersteller einer Hauptplatine zusammen mit dem TPM eingebaut. Klar ist, dass dabei beispielsweise

BIOS Updates ausschließlich über gesicherte, vom Hersteller genau festgelegte Wege erfolgen dürfen.

Über ein „Measurement Log“, das genau protokolliert, welche Hardware bzw. Systeme gestartet wurden, kann der Zustand des Systems sichergestellt werden. Das Log beinhaltet nicht nur die Art sondern auch die Reihenfolge, in der einzelne Komponenten ausgeführt wurden.

Grundlage der Spezifikation ist die Tatsache, dass sowohl das TPM als auch das CRTM als vertrauenswürdig und unveränderbar angesehen werden. Diese beiden Teile werden zum „Trusted Building Block“ (TBB) zusammengefasst. In diesen TBB greift auch der Mechanismus „Physical Presence“ ein, der beweisen soll, dass der Benutzer tatsächlich physikalischen Zugriff auf das System hat (z. B. durch Drücken einer speziellen Taste am Gehäuse). Dies ist eine reale Interaktion des Benutzers mit diesem Modul. (Beispiel für die Notwendigkeit ist die Löschung des TPMs bzw. wenn der Besitzer das TPM freigeben möchte, um z. B. die Hardware weiterzugeben.)

Basierend auf diesem originären Startpunkt des Vertrauens wird während des Bootvorgangs eine Vertrauenskette bis hin zum Betriebssystem aufgebaut, die über das Measurement Log und die Werte in den Platform Configuration Register des TPM überprüft werden kann. Zu den überprüfbaren Teilen gehören auch die Daten von Grafikkarten, PCI-Karten oder anderen Hardwarekomponenten. Diese Spezifikation legt auch fest, mit welchen Daten genau die PCR geladen werden sollen.

2.3.2.4 Server Work Group

Die Arbeit der Server Work Group basiert grundsätzlich auf den Spezifikationen der PC Client Work Group, erweitert bzw. spezialisiert diese allerdings auf den Einsatz in Servern. Generell ist vorgesehen, dass als Grundvoraussetzung ein TPM benutzt wird, das einem TPM aus der Client-Umgebung gleicht – es könnte allerdings auch ein TPM entwickelt werden, das mit gleichen Funktionen ausgestattet auch eine höhere Bandbreite bietet (beispielsweise beim Einsatz von Hashing oder der Verschlüsselung) und somit als Crypto-Hardware für den Servereinsatz dienen kann.

Desweiteren kommt bei Servern (insbesondere Mehrprozessorsystemen) häufig das Konzept der Virtualisierung bzw. Partitionierung zum Tragen. Aus einem physikalischen Stück Hardware werden mehrere logische Server erzeugt, die relativ unabhängig voneinander existieren und unterschiedliche Aufgaben übernehmen, ja auch mehrere Betriebssysteme beherbergen können.

Hier ist es notwendig, jedem virtuellen Server eine oder auch mehrere physikalische TPMs zuordnen zu können. Der Zugriff auf ein TPM darf nur von vorher per „Binding" fest verbundenen Partitionen erfolgen. Dabei kann das „Binding" physikalisch – also durch eine feste Verdrahtung – oder logisch über eine kryptographische Bindung erfolgen. Die verschiedenen Measurements aus den PCRs müssen allerdings auf allen TPMs zur Verfügung stehen.

Ein Vorschlag der Spezifikation ist, statt vieler einzelner TPMs für alle Partitionen einen einzigen Endorsement Key zu verwenden. Alle anderen Attribute müssen aber einzigartig für die Partition sein (z. B. der Storage Root Key), um sicherzustellen, dass die Attestation Keys eines Systems nicht von anderen Systemen aus zugänglich sind.

2.3.2.5 Storage Work Group

Von der Arbeitsgruppe, die sich mit dem Bereich Speichersysteme beschäftigt, ist bisher (Stand November 2006) lediglich eine "Use Case Whitepaper" verfügbar. Dieses Paper beschäftigt sich mit verschiedenen Sicherheitsproblemen, die im Bereich der Speicherung von Daten auftreten. Ziel der Arbeitsgruppe soll sein, entsprechende Spezifikationen für die beschriebenen Probleme zu erarbeiten.

So wird das Problem diskutiert, wie sichergestellt werden kann, dass z. B. eine Festplatte nach dem Austausch, Verkauf oder evtl. Diebstahl nicht vom Folgebesitzer ausgelesen werden kann. Dies ist gerade auch in großen Data Centers ein Problem, wenn große Systeme ersetzt werden.

Hier wird allerdings nicht (wie vielleicht offensichtlich) erwägt, in jede Festplatte ein TPM einzubauen – die Storage Work Group schlägt vielmehr Erweiterungen zu den existierenden SCSI- und ATA-Befehlen vor, die für mehr Sicherheit sorgen sollen.

Zu den Vorschlägen gehört auch „Host-to-SD mating“, also die direkte Koppelung eines Hosts an ein Speichergerät – und umgekehrt.

Ähnlich dazu ist die Überlegung, einzelne Bereiche eines Speichersystems gezielt an einen Host bzw. eine Applikation zu binden. Weitere Überlegungen beinhalten die Verschlüsselung von Daten (vgl. 2.2.2.2 Auslagerung (Binding)), das erweiterte Logging von Sicherheitsverstößen auf Hardwareseite sowie der mögliche sichere Download von Firmware auf Speichersysteme).

2.3.2.6 Trusted Network Connect

Die Sicherheit und Zuverlässigkeit verteilter Systeme zu erhöhen ist Ziel der Arbeitsgruppe “Trusted Network Connect”. Viren, Würmer und DOS-Attacken sollen eingedämmt werden, indem Administratoren die Möglichkeit haben, Endgeräte zu überprüfen, bevor sie sich mit dem Netz verbinden. Grundidee ist, dass in einer idealen Umgebung nur Systeme, die einer definierten Sicherheitsvorschrift (Security Policy) entsprechen, Zugang zum Produktivnetzwerk haben. So soll es jederzeit möglich sein, den Zustand von am Netzwerk beteiligten Systemen (Clients, Netzwerkgeräten, …) zu überwachen und evtl. einzuschränken oder zu deaktivieren, wenn ein Verstoß festgestellt werden kann. Dies könnten z. B. durch Angriffe beeinträchtigte Netzwerkgeräte sein, oder auch Clients, deren Anti-Virensoftware nicht dem neuesten Stand entspricht. Solche Geräte könnten dann im Netz isoliert werden, bis z. B. Updates installiert wurden und können danach am Netzwerk teilnehmen. Somit ist ein Grundvertrauen in Geräte, die im Netzverkehr beteiligt sind, generell höher.

Security Requirements	Interoperability Standards
▪ Permit only authenticated users and devices to connect to the network	▪ IEEE 802.1x, IETF RADIUS, IETF EAP
▪ Enable administrator to establish security policies for anti-virus, patch levels, software versions, etc.	Focus of TCG Efforts
▪ Measure device configuration against security policies before its connection to the network is allowed	
▪ Identify devices that are not compliant	
▪ Quarantine non-compliant devices	
▪ Remediate non-compliant devices to ensure compliance to security policies	

Abbildung 4: Einsatzgebiete von TNC

Quelle : Whitepaper „Trusted Network Connect to Ensure Endpoint Integrity", Seite 2

Hier setzt die TCG bzw. Work Group TNC nicht einzig und allein auf die Konzepte mit einem Trusted Platform Module. Ziel ist auch, einheitliche Standards zu schaffen, die herstellerunabhängig die geforderten Möglichkeiten bieten, dass Geräte Metadaten untereinander austauschen können. Die notwendigen Anforderungen an die Kommunikation werden in den Interface-Spezifikationen der TCN Work Group beschrieben und festgelegt. Dabei werden die existierenden Standards IEEE 802.1x und IEFT EAP wenn notwendig erweitert.

TPMs sind in dieser Spezifikation nicht zwingendermaßen erforderlich, um die vertrauensvolle Verbindung von Geräten aufzubauen. Allerdings soll das bereits im Teil 2.3.2.3 PC Client beschriebene Konzept der Measurements die Vertrauenswürdigkeit der Angaben eines Gerätes erhöhen und die Verwendung von TPMs wird somit von der Arbeitsgruppe empfohlen.

2.3.3 Vertrauenswürdige Betriebssysteme

Mehrere Gruppen haben es sich zur Aufgabe gemacht, basierend auf den Spezifikationen der TCG die dazugehörigen sicheren Betriebssysteme zu entwickeln. Diese sollen in diesem Kapitel näher betrachtet werden.

2.3.3.1 Microsoft - von Palladium über NGSCB zu BitLocker

Entwicklung

Die Firma Microsoft ist Gründungsmitglied der TCPA sowie der TCG und somit seit Beginn an den Entwicklungen der TCG beteiligt. Ihre Entwicklungsvorhaben im Bereich der Betriebssysteme unter Berücksichtigung der TCG Spezifikationen wurden mit Beginn der TCG im Jahr 2002 unter dem Codenamen Palladium bekannt.

Das Projekt wurde bald in NGSCB („Next Generation Secure Computing Base") umbenannt. Ob dies wegen eines möglicherweise drohenden Markenrechtsstreits erfolgte oder wegen der Tatsache, dass „Palladium" recht bald mit einem schlechten Image belegt war, wurde von Microsoft nicht kommentiert.

Der Grundgedanke von NGSCB ist, dass es anstatt einer herkömmlichen Umgebung, in der ein Betriebssystem läuft, zwei getrennte Abteilungen gibt. Während auf der nicht vertrauenswürdigen sog. linken Seite eine Windows Installation ‚wie bisher' läuft, ist die sog. rechte Seite die vertrauenswürdige. Diese Umgebung trägt den Namen „Nexus" und basiert auf dem TCG-Design also einem Trusted Platform Module und dem darauf aufbauenden sicheren Bootvorgang.

Während im linken Teil bisherige Applikationen auf den vollem Umfang der Windows API zurückgreifen können und daher in vollem Umfang kompatibel sein sollen, setzt der Nexus voraus, dass hier lauffähige Applikationen neu entwickelt werden. Die verfügbare API im Nexus soll schlanker sein. Im Gegensatz zu der mittlerweile komplexen Windows API soll so die Überwachbarkeit des Codes und das Überprüfen auf Fehler leichter fallen. Dabei muss eine Applikation nicht komplett im rechten Teil laufen, sondern der sicherheitsrelevante Teil (sog. NCA – Nexus Computing Agent) kann auf gesicherten Pfaden auf den im unsicheren Modus laufenden Teil der Anwendung zugreifen. Die Schnittstelle zwischen den beiden Teilen wird dabei genau überwacht.

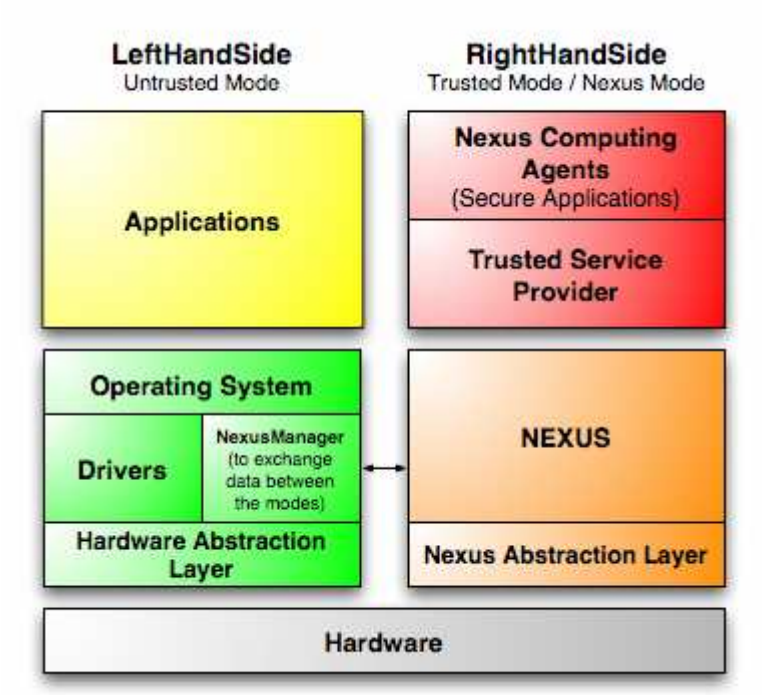

Abbildung 5: NGSCB Architektur

http://en.wikipedia.org/ - Artikel NGSCB, Stand 17:05, 31 Oktober 2006

Die Trennung der Speicherbereiche wird dabei auch hardwareseitig überwacht. Aktuelle CPUs und das TPM zusammen können sog. „Curtained Memory" bereitstellen. Dieser Speicherbereich ist ausschließlich der Applikation zugänglich, die den Speicher zugeordnet bekommen hat. Dies kann auch über die kryptografischen Methoden des TPM gesichert werden. Diese Speicherbereiche sind somit für Methoden des Reverse Engineerings oder unerlaubten Zugriff nicht zugänglich.

Dieses Gesamtkonzept erfordert, dass vertrauenswürdige Software für die Nexus API neu entwickelt werden muss. Ebenso muss eine Zertifizierungsstrategie dafür sorgen, dass diese Software den Sicherheitsansprüchen entspricht und ‚vertrauenswürdig' abläuft.

Heutiger Stand von NGSCB

Dieses Architekturkonzept wurde von Microsoft ursprünglich zusammen mit Windows „Longhorn" (heute Vista) für das Jahr 2004 angekündigt. Nachdem Vista immer weiter verschoben wurde, kündigte Microsoft im Mai 2005 das NGSCB-Konzept ab[3].

[3] http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=18841713 (2006-12-07)

Zuverlässige Informationen zu diesem Thema sind schwer zu finden. Die offizielle Webseite von Microsoft zum Thema NGSCB[4] ist veraltet. Sie informiert noch über „Longhorn", währende weiterführende Links auf Informationen aus dem Juli 2003 oder allgemeine Seiten – die nicht weiter auf NGSCB eingehen – verweisen. Einige der verlinkten Seiten sind nicht mehr existent und die angegebene E-Mail-Adresse für alle Anfragen ist nicht mehr erreichbar.

Realisierungen

Teile des Konzepts sollten in Vista implementiert werden, was zum heutigen Zeitpunkt z. B. der so genannte „Secure Startup" bzw. BitLocker ist. Mit BitLocker ist es möglich, unter den Windows Vista Versionen Enterprise und Ultimate die Festplatte des Betriebssystems oder auch andere Datenträger zu sichern. Dabei werden drei Möglichkeiten des Verschlüsselns angeboten, von denen zwei die Benutzung und das Vorhandenseins eines TPM 1.2 erfordern, während die dritte Methode mit einem USB-Stick arbeitet und auch ohne TCG-konformes System arbeitet.[5]

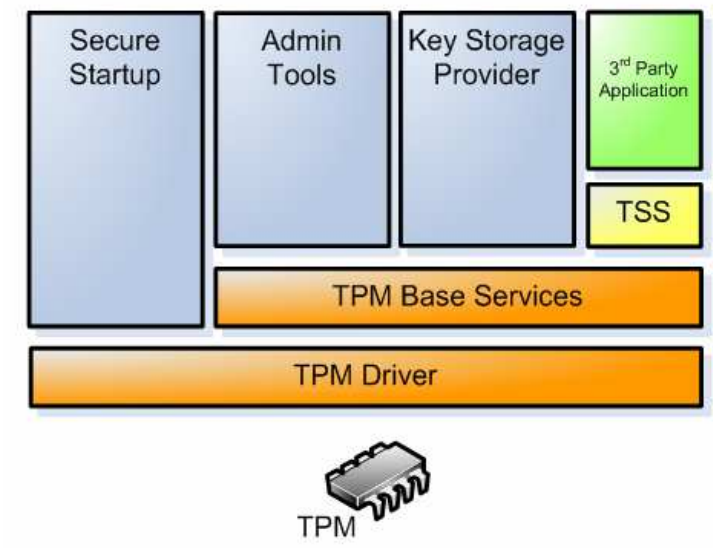

Abbildung 6: Vereinfachte Architektur der TPM Services in Windows Vista

Quelle: Trusted Platform Module Services in Windows Vista (Apr 25, 2005)
http://www.microsoft.com/whdc/system/platform/pcdesign/TPM_secure.mspx

---

[4] http://www.microsoft.com/resources/ngscb/
Keywords: microsoft ngscb

[5] http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx - Technische Details zu BitLocker
Keywords: technet bitlocker drive encryption

Die TPM Administration Tools erlauben es Administratoren größerer Netzwerke zu definieren, welche Funktionen eines TPM auf einer bestimmten Maschine ausgeführt werden dürfen, um z. B. die Freigabe persönlicher Daten eines Benutzers zu sperren.

Der Key Storage Provider erlaubt Applikationen den Zugriff auf die Funktionen des TPM. Einfache Krypto-Operationen oder die Verschlüsselungs- und Signierungsmethoden des TPM können so angesprochen werden.

Mit der Veröffentlichung weiterer Informationen zu diesen Themen hält sich Microsoft bedeckt. Welche weiterführenden Ziele gesteckt wurden, lässt sich momentan nicht absehen. (vgl. 5.2.2 Windows Vista)

2.3.3.2 OpenTC – Open Trusted Computing

Die Entwicklung eines sicheren Betriebssystems, basierend auf der von der TCG beschriebenen Technologie, ist das Ziel des Projekts OpenTC[6]. Ein Zusammenschluss aus mehreren Firmen und Universitäten (darunter HP, IBM, Infineon, SuSE sowie TU Dresden, TU München, University of Cambridge) erarbeitet praktisch ein Framework, um ein sicheres Betriebssystem, dazugehörige Protokolle und Software sowie Beispielapplikationen zu entwickeln.

Das Projekt versteht sich selbst als Entwicklungsprojekt, das die eventuellen Hürden bei der Implementierung der TCG Spezifikationen klären möchte. Dabei ist interessant, dass die Arbeit als OpenSource veröffentlich wird und auch von den Entwicklern keine Probleme in der (Un-)vereinbarkeit von Trusted Computing UND OpenSource gesehen werden, was im Zusammenhang mit TC viel diskutiert wird.

Die von der TCG erarbeiteten Spezifikationen einer „sicheren Hardware“ dienen als Basis, auf der Schicht für Schicht das sichere Betriebssystem aufbaut. Darüber liegende Schichten wie der TSS (2.2.3 TSS – Trusted Software Stack) werden entwickelt, darunter der dazugehörige Trusted Service Provider, der als weiteres Ziel

[6] http://www.opentc.net/ Informationen zu OpenTC (2006-12-17)

des Projektes bekannten Paketen wie OpenSSL oder OpenSSH für die Krypto-Operationen zur Verfügung steht und diese von der Hardware durchführen lässt.

Ziel ist, ein fertiges System zur Verfügung stellen zu können, sobald auch proprietäre Betriebssysteme auf dem Markt verfügbar sind – und dies nicht nur für PCs, sondern auch im Bereich der Mobiltelefone, Server und ähnlichen Plattformen.

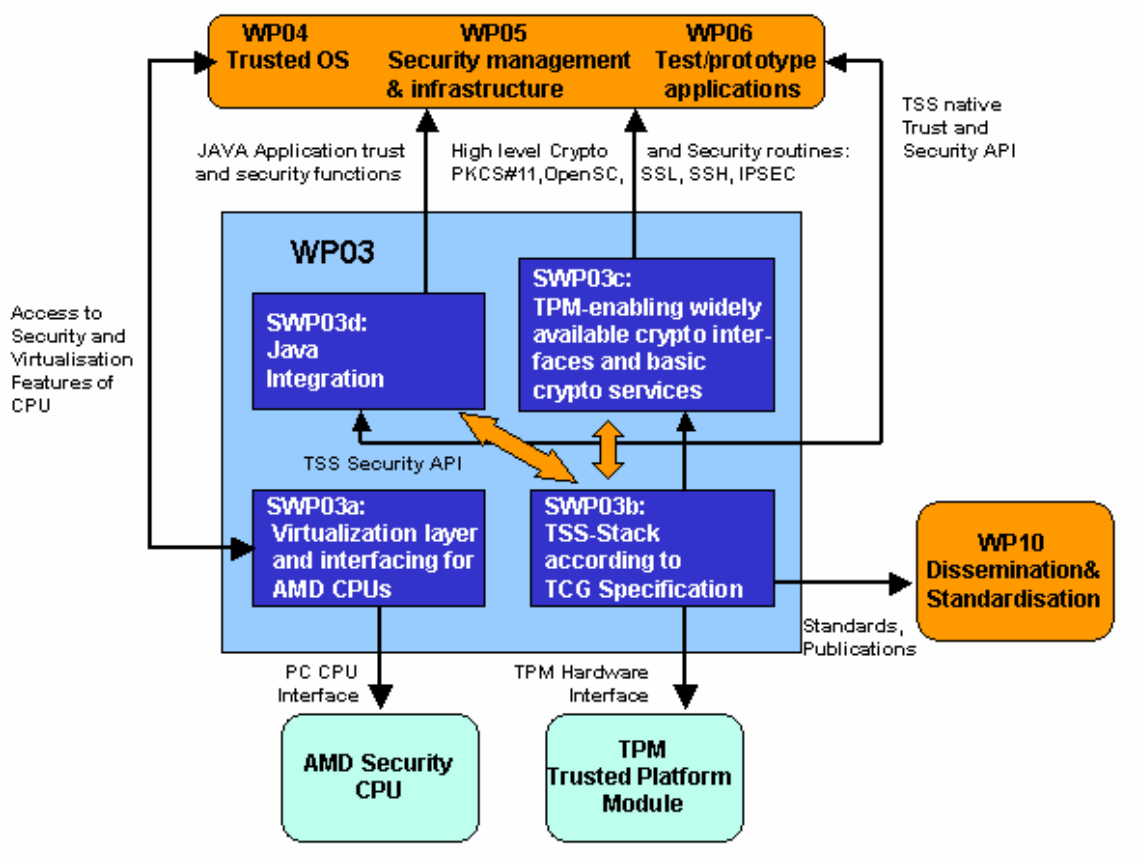

Abbildung 7: Trust Layers (OpenTC)

Quelle: http://www.opentc.net/info/activitiesWP03 (2006-12-17)

2.3.3.3 Turaya – EMSCB

„Das Projekt European Multilaterally Secure Computing Base (EMSCB) entwickelt eine vertrauenswürdige Plattform mit offenen Standards, die viele Sicherheitsprobleme herkömmlicher Plattformen löst."[7]

Die Sicherheitsarchitektur wird in einer praktischen Umsetzung, dem Projekt „Turaya", als OpenSource realisiert und hat zum Ziel, basierend auf einer nicht-

[7] http://www.emscb.de/

proprietären Plattform die Funktionalitäten eines TPM zur Verfügung zu stellen. Dabei soll die Umsetzung keine Erweiterung eines Betriebssystems sein, sondern durch eine Art Virtualisierung ein Umgebung schaffen, in der ein beliebiges Betriebssystem parallel zu den sicheren Applikationen laufen kann.

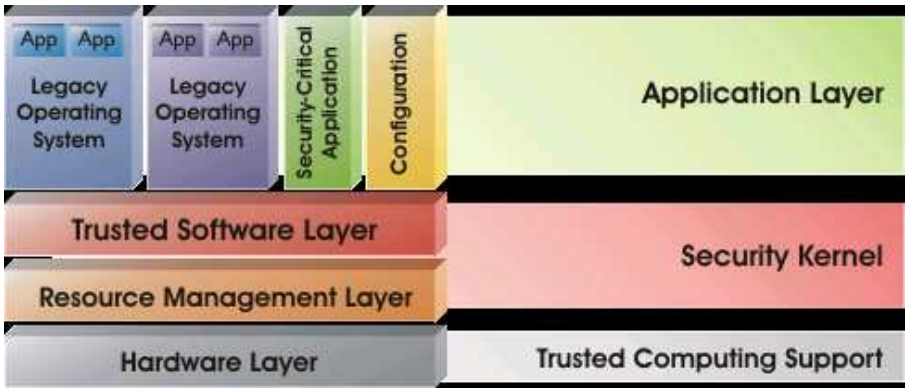

Abbildung 8: Architektur von Turaya

http://www.internet-sicherheit.de/trusted-computing.html

Dabei ist der User selbst in der Lage, den Zugriff auf die Hardware zu kontrollieren und dem in der virtuellen Umgebung laufenden Betriebssystem Einschränkungen aufzuerlegen oder nicht. Lokale Sicherheitsrichtlinien des Benutzers lassen sich so durchsetzen.

Durch die Verlagerung des Betriebssystems in den – aus Sicht der EMSCB – Appliation Layer, können alle Anwendungen wie bisher in dieser als unsicher betrachteten ‚gewohnten' Umgebung laufen. Im parallel im Application Layer liegenden Bereich der sicheren Anwendungen können Turaya-spezifische, gesicherte Applikationen ablaufen. Diese haben die Möglichkeit, auf sicheren Kanälen mit dem Betriebssystem zu kommunizieren.

Vorangetrieben wird das Projekt von der Ruhr-Universität Bochum, der Fachhochschule Gelsenkirchen, der Technischen Universität Dresden, der Sirrix AG security technologies und der escrypt GmbH sowie mit Unterstützung durch das Bundesministerium für Wirtschaft und Technologie. Es wurden exemplarisch bereits zwei sichere Applikationen veröffentlicht: Turaya.Crypt ermöglicht, Speichermedien

transparent zu verschlüsseln und Turaya.VPN bietet die Möglichkeit, transparente, hardwareseitig unterstützte VPN-Tunnel aufzubauen.

Das Konzept ist vergleichbar mit dem Konzept NGSCB von Microsoft (vgl. 2.3.3.1 Microsoft - von Palladium über NGSCB zu BitLocker), allerdings werden die vorgesehen Möglichkeiten der Sicherheitsregelungen durch den Benutzer laut des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen (http://www.internet-sicherheit.de/trusted-computing.html) in NGSCB so nicht vorgesehen. Desweiteren kann EMSCB mit einem TPM als auch zukünftigen Technologien für Trusted Computing verwendet werden.

2.3.4 Beispielanwendung HP ProtectTools Embedded Security

Verschiedene Hersteller bauen seit einiger Zeit die TPMs schon in ihre Notebooks oder PCs ein und bieten – auf Basis eigener Softwareapplikationen – Funktionalitäten mit dem TPM an. So war es möglich, auf einem HP Notebook NX6325 mit integriertem TPM 1.2 einige dieser Funktionen zu testen. Die Anwendung „HP ProtectTools Embedded Security“[8] läuft unter Windows XP Home und bietet nach erfolgter Besitzübernahme des TPMs durch den Administrator und der Erstellung eines Passwortes für den Benutzer mehrere Funktionen an.

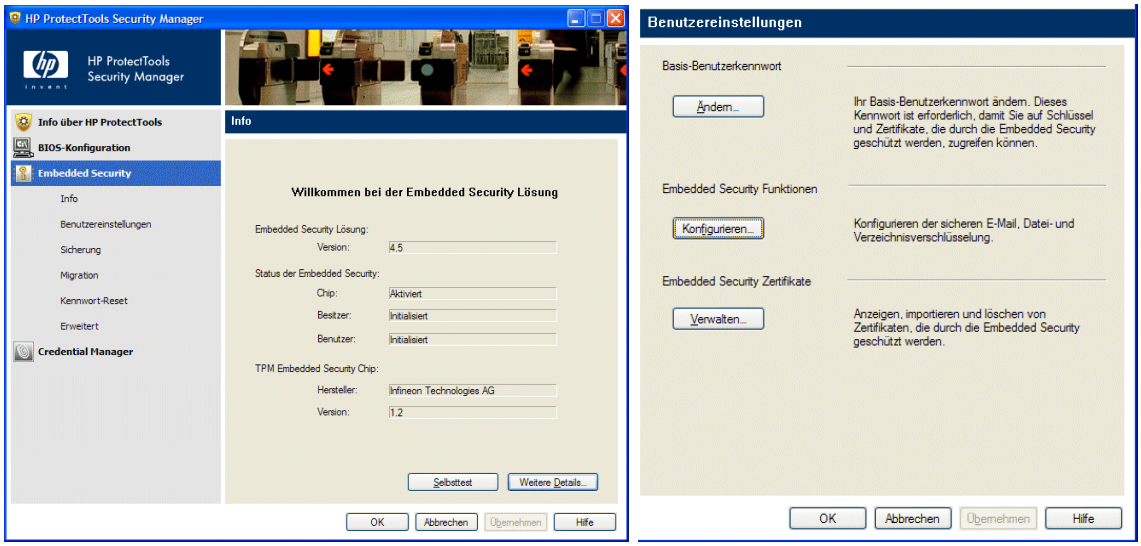

Abbildung 9: HP ProtectTools - Embedded Security

[8] www.hp.com/hps/security/products/ HP ProtectTools
Keywords: hp protecttools security solutions

Die für den Benutzer verfügbaren Anwendungen beschränken sich in dieser Version auf Grundfunktionen. Die Verwaltung bzw. Sicherung von Zertifikaten für den sicheren Mail-Verkehr wird angeboten. Eine weitere Anwendung ist ein „Personal Secure Storage“: Hier wird für den Benutzer ein virtuelles Laufwerk wählbarer Größe angelegt, das über das TPM verschlüsselt wird und sich für andere Benutzer lediglich als verschlüsselte Datei zu erkennen gibt. (Beispiel für 2.2.2.2 Auslagerung (Binding))

3 Digital Rights Management

3.1 Begriffsdefinition

Digitale Daten können verlustfrei von einem Datenträger zum anderen kopiert werden und somit einer großen Anzahl von Benutzern zur Verfügung gestellt werden. Diese Tatsache wird dann zu einem unerwünschten Problem, wenn es sich um rechtlich geschützte Daten handelt, deren Nutzung vom Urheber oder Eigentümer der Daten eingeschränkt werden soll. Diese Einschränkung liegt besonders im Interesse der Musik- und Filmvertreiber und soll mittels digitaler Rechteverwaltung (Digital Rights Management – DRM) erreicht werden.

Eines der Grundprinzipien von DRM ist, dass Daten (z. B. eines Musikstückes) in verschlüsselter Form vorliegen und der Konsument zum Abspielen dieser Daten nicht nur eine geeignete Software (Player) sondern auch den Schlüssel bzw. ein Zertifikat oder eine Lizenz besitzen muss.

Diese Lizenz regelt in den meisten Fällen nicht nur, ob das Stück prinzipiell gespielt werden darf, sondern beinhaltet dabei auch je nach Anwendungsbereich weitere Einschränkungen. So kann z. B. geregelt werden, wie oft ein Stück auf CD gebrannt werden darf, ob die Daten auf einem tragbaren Gerät benutzt werden dürfen oder – im Bereich der digitalen Schriftstücke – ob Textpassagen kopiert werden dürfen oder nicht.

DRM basiert also auf einer Trennung der ‚Nutzdaten' und der Zugangsberechtigung zu den Daten. Wie erwähnt ist es möglich, die Rohdaten verlustfrei zu kopieren, deren Verwendung ist allerdings eingeschränkt, da sie ohne Lizenz nicht zugänglich sind.

3.2 Ursprung

Erste Gedanken in dieser Richtung, also der Trennung von Nutzdaten und deren Rechteinhabern, finden sich in Mark J. Stefiks Artikel „Letting Loose the Light: Igniting

Commerce in Electronic Publication“ [9] Er stellt ein Konzept vor, das auf zwei Ideen beruht, die beim Umgang mit geschütztem Material vorausgesetzt werden:

- Digitale Werke können zwischen „Trusted Systems“ gehandelt werden.
- Die Beschreibungen ihrer Nutzungsrechte und deren Nutzungskosten sind mit den Werken verbunden.

In seinem Artikel beschreibt Stefik mehrere Szenarien, wie dieses System arbeiten soll. Die „Trusted Systems“ verweigern jegliche nicht lizenzierte Kopie, verlangen Gebühren für die Nutzung oder Weitergabe und ermöglichen auch die temporäre Nutzung eines Werkes (Verleih) bis zu einem bestimmten Zeitpunkt, sprechen währenddessen allerdings dem Verleiher die Nutzungsrechte ab.

Die nutzungsabhängige Abrechnung der Daten wird in seinem Artikel ebenso beschrieben. Dabei geht er auf unterschiedliche Modelle ein wie zeitabhängige Bezahlungsmodelle für Musik oder auch die Unterscheidung zwischen Büchern, die man eventuell einmalig komplett liest oder anderen Werken wie Enzyklopädien, die nur gelegentlich benutzt werden.

Er stellt in seinem Konzept auch Lizenzen vor, die einem Nutzer gewisse Verwendungen der Werke zugestehen und spricht von einer „digital Authority“, einem Authorisierungsserver der diese Lizenzen zentral überwacht.

Stefik erwähnt in seinem Artikel auch die Grenzen dieser Technologie. Zum einen basiert das System darauf, dass alle „Trusted Systems“ integer sind, also nicht umgangen werden können und es nicht möglich ist, die Daten verlustfrei aus dem geschlossenen System zu lösen.

Zum anderen wird es durchaus möglich sein, Texte abzuschreiben oder Ausdrucke anderweitig zu kopieren bzw. auch Musik über ein Mikrophon wieder neu

[9] Letting Loose the Light: Igniting Commerce in Electronic Publication. In: Stefik, M., ed. Internet Dreams: Archetypes, Myths, and Metaphors, MIT Press, Cambridge, MA, 1996

aufzunehmen. Von den möglichen Qualitätsverlusten abgesehen, erwähnt Stefik interessanterweise hier schon die Möglichkeit, versteckte Zusatzdaten in die Werke einzubringen, also unsichtbare oder unhörbare Informationen einzubauen, die eine Zurückverfolgung des Ursprungs zulassen.

Trotz dieser Einschränkungen sieht Stefik in seinem Konzept den Anreiz, dass mehr Menschen die Möglichkeit haben, mit ihren Werke Geld zu verdienen und somit mehr Werke veröffentlich würden. Diese würde Kreativität fördern – „Letting Loose the Light".

3.3 Funktionsweise

Dieses Kapitel zeigt die diversen Formen des Digital Rights Managements in verschiedenen Anwendungsbereichen

3.3.1 DRM im Offline Bereich

Um zu verhindern, dass geschützte Daten ohne entsprechende Berechtigung zugänglich gemacht werden können, sind diese in einer dem System angemessenen Form verschlüsselt. Je nach Anwendungsgebiet und der Möglichkeit, Berechtigungen online und Nutzer-basiert zu überprüfen oder nicht, werden verschiedene Methoden der Ver-/Entschlüsselung eingesetzt. So sind beispielsweise Film-DVDs mit dem Verschlüsselungsschema CSS (Content Srambling System) verschlüsselt. Da es für DVD-Player nicht möglich ist, eine (Online-)Authentisierung des Benutzers durchzuführen, hat man mit CSS die Dekodierung der Daten nur lizenzierten und zertifizierten Geräten/Herstellern ermöglicht. Die Algorithmen und Zertifikate sind rein in der Hardware des Gerätes enthalten und somit vermeintlich nicht angreifbar. Man verlässt sich hier auf integere Endgeräte, geschlossene Systeme, die den ausgehenden Datenstrom z. B. nur über die verlustbehafteten analogen Ausgänge eines Geräts ausgeben, damit ein digitales Wiederaufzeichnen der Daten nicht möglich ist.

3.3.2 DRM im Online Bereich

Für Daten, die über DRM im Internet oder Firmennetz geschützt werden, ist meist der Kontakt zu einer Autorisierungsstelle notwendig. Über einen zentralen Server werden

über die Zugangsdaten des Benutzers die Berechtigungen für den Zugriff auf bestimmte Daten freigegeben oder verhindert.

Um der Applikation mitzuteilen, an welcher Stelle oder Adresse die Überprüfung der Zugangsdaten stattfindet, sind die verschlüsselten Nutzdaten je nach Format noch mit zugänglichen, beschreibenden Metadaten versehen. Diese Daten beinhalten z. B. die Informationen über den Eigentümer der Daten oder des Urhebers und eine URL, an der die Zugriffsberechtigung verwaltet wird.

Wie schon Stefik in seinem Artikel beschrieben hat, geht es dabei aber nicht nur um die reine Entscheidung, ob jemand die Daten sehen bzw. hören o. ä. darf, sondern es werden meist auch weitere Aktionen eingegrenzt wie die Möglichkeit, Textstellen zu kopieren, Musik auf CD zu brennen, auf tragbare Geräte zu portieren, auf mehr als einem System zu benutzen usw. Voraussetzung ist hierbei, dass die Applikation, die dem Nutzer die Daten zur Verfügung stellt, ebenfalls integer ist.

Sollte ein Gerät oder eine Software Zugriff auf die Daten bekommen, dabei die Daten allerdings nicht im Sinne der lizenzgebenden Stelle verwenden sondern freigeben, so ist der Schutz wirkungslos. Aus diesem Grunde werden für die meisten DRM-Systeme nur bestimme Applikationen als Schnittstelle zum Lizenzserver zugelassen.

3.3.3 DRM im mobilen Bereich

3.3.3.1 Tragbare Abspielgeräte

Bei Anwendungen, die das Kopieren der Daten auf andere Medien erlauben, wird dies meist ebenfalls allein durch die entsprechende Applikation erlaubt. So können DRM geschützte Musikstücke meist nicht per herkömmlicher Anwendung zum Erstellen von CDs gebrannt werden, sondern dafür kann nur der zum DRM System gehörende Player/Reader verwendet werden. Dieser hat dadurch die Möglichkeit, zu protokollieren, wie oft ein Musikstück vervielfältigt wurde und kann dies gegebenenfalls unterbinden, wenn die in der Lizenz vorgesehene Anzahl von Kopien erreicht ist. Gleiches gilt für das Synchronisieren von Daten (Musik, Video, aber auch eBooks) auf tragbare Geräte wie PDAs oder MP3-Player.

Bei den meisten gängigen Systemen (siehe 3.4 DRM-Systeme), die Unterstützung für tragbare Geräte bieten, werden die mobilen Applikationen an einen Host bzw. ein Benutzerkonto gebunden. So ist es oftmals notwendig, die Geräte zu ‚aktivieren', was einer Verknüpfung sowohl mit dem Daten liefernden Host und einer Benutzerkennung entspricht. Gerade bei tragbaren Musik-Playern, die über keine eigene Verbindung zum Internet verfügen, ist der Host als Datenlieferant erforderlich (wobei die Verbindung über USB, Bluetooth, Firewire, usw. hergestellt wird).

Dabei wird z. B. die Kennung des Benutzers, die bereits mit der auf dem Rechner laufenden Applikation verknüpft wurde, auf das mobile Gerät kopiert. Somit können nur von dem entsprechenden Nutzer erworbene Stück abgespielt werden. Dies macht allerdings eine Synchronisierung des mobilen Gerätes mit einem anderen Host unmöglich. Es ist somit meist nicht möglich, Musikstücke zweier verschiedener Nutzerkonten auf einem mobilen Gerät zu hören.

Ebenso führt ein Synchronisierungsversuch mit einem zweiten Rechner oftmals dazu, dass eine Löschung des mobilen Gerätes angeboten bzw. vorausgesetzt wird, um neue Daten eines anderen Nutzers aufzuspielen.

Allerdings ist es hingegen oftmals möglich, mehrere mobile Geräte mit einem Benutzerkonto bzw. Host zu verbinden und somit ein einmal erworbenes Musikstück auf alle ‚eigenen', also direkt an das Benutzerkonto gebundenen Abspielgeräte zu kopieren.

3.3.3.2 DRM im Bereich der Mobiltelefone

Im stark wachsenden Markt der Klingeltöne für Mobiltelefone gibt es zwei Prinzipien, um die Weitergabe von DRM-geschützten Inhalten von einem Gerät auf das andere zu verhindern. Neuere Geräte, die über leistungsfähigere Prozessoren und Betriebssysteme sowie weitergehende Funktionen verfügen, benutzen mittlerweile gleiche DRM-Systeme wie andere Geräte, z. B. PDAs und tragbare MP3-Player. D.h. hier kommen ebenfalls Systeme zum Einsatz, die eine Bindung der Nutzdaten an das

Gerät oder auch die Telefonnummer des Benutzers (somit einem eindeutigen Benutzerkonto vergleichbar) verwenden.

Ältere Modelle erlauben es von Geräteseite nicht, auf die herunter geladenen Daten über integrierte Funktionen der Weitergabe von Endgeräte zu Endgerät, wie z. B. über Bluetooth oder Infrarot, zuzugreifen. So sind diese Dateien je nach Gerät entweder als geschützt gekennzeichnet und jegliche Funktionen der Weitergabe sind deaktiviert, oder die Daten sind für den Benutzer bei Suchen in der Dateistruktur des Mobiltelefons (z. B. mit integrierten Datei-Browsern, bei Bluetooth-Verbindungen per OBEX-File-Transfer oder über kabelgebundene Zugriffe) nicht sichtbar. Dieser Mechanismus setzt also wiederum auf integere Endgeräte, denn die geschützten Daten sind nicht verschlüsselt, aber der Zugriff soll dem Benutzer durch den Gerätehersteller verweigert werden.

3.4 DRM-Systeme

Die heutigen DRM-Systeme finden sich hauptsächlich in zwei Bereichen: Dem Medienbereich zum Schutz von urheberrechtlich geschützten Inhalten wie Musik, Filmen und Büchern sowie dem Einsatz in Unternehmen zum Schutz und zur Zugriffskontrolle für sensible Daten.

3.4.1 Audio/Video-Bereich

Die folgende Liste erhebt keinen Anspruch auf Vollständigkeit, allerdings sollen die meist verbreiteten DRM-Systeme exemplarisch genannt werden.

3.4.1.1 Windows Media DRM – PlaysForSure – Microsoft

Seit April 1999 ist Windows Media DRM verfügbar und wird für Musik- und Videodateien eingesetzt. Das System arbeitet mit den Formaten WMA (Windows Media Audio) und WMV (Windows Media Video), die mittlerweile in mehreren Versionen verfügbar sind. Die aktuelle Version 10 des Windows Media DRM bietet in Zusammenarbeit mit dem Windows Media Player verschiedene Möglichkeiten, wie Lizenzen gehandhabt werden können.

Bei jedem Abspielvorgang wird überprüft, ob für eine Mediendatei die gültige Lizenz im lokalen Lizenzspeicher des Systems vorhanden ist. Sollte dies nicht der Fall sein,

so wird mit dem im Header der Datei angegebenen Lizenzierungsserver Kontakt aufgenommen und versucht, eine Lizenz zu erhalten. Diese Lizenz kann dann je nach Voraussetzung direkt erteilt werden („silent“) oder wird z. B. durch Öffnen eines Browsers erst nach Bestätigung, Eingabe von Nutzerdaten oder evtl. Freigabe durch ein Shopping-System erteilt („non-silent“). Ein Ablaufdatum der Lizenzen, z. B. für monatliche Abonnements oder begrenzte Vorschau-Angebote ist dabei ebenso berücksichtigt wie die Möglichkeit, für ein Musikstück mehrere verschiedene Lizenzen anzubieten und diese getrennt zu verwalten.

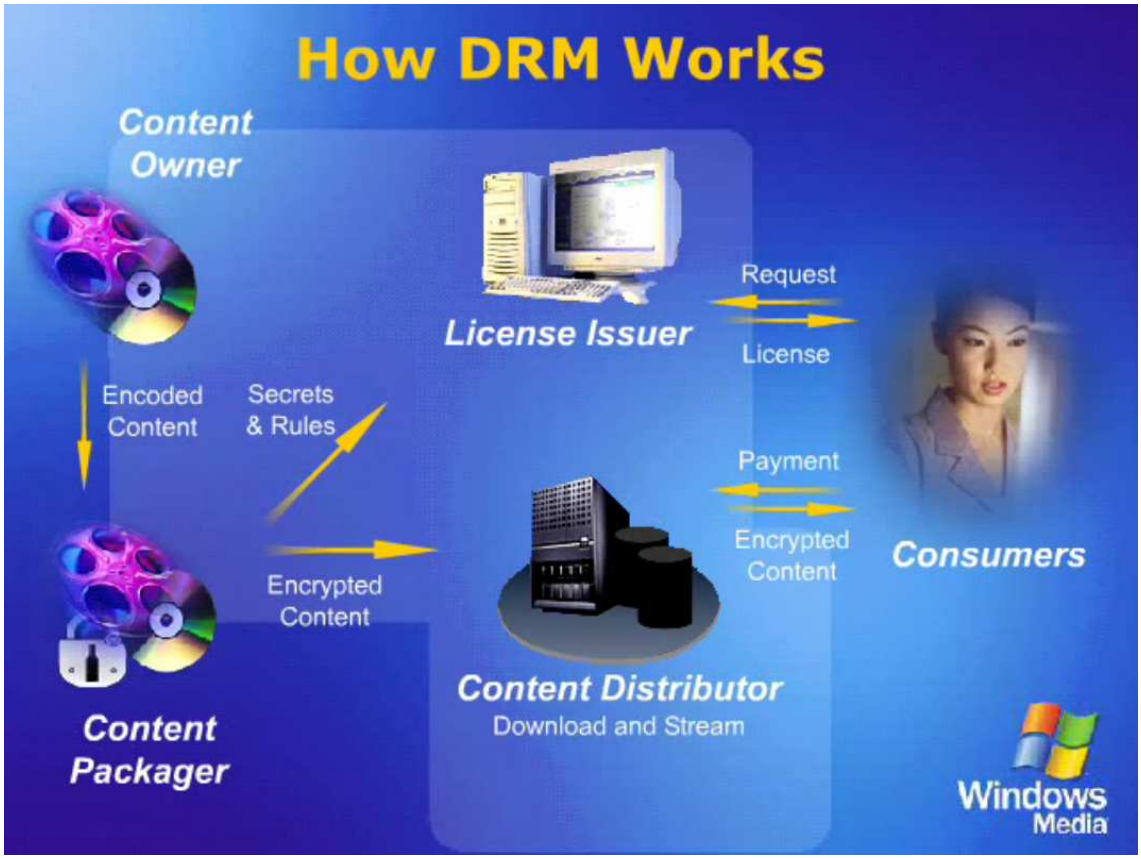

Abbildung 10: Windows Media DRM Überblick

Quelle: Aus „Encrypting Content“, Video Tutorial
http://www.microsoft.com/windows/windowsmedia/forpros/drm/tutorial.aspx

Dadurch ist es auch möglich, Lizenzen im Nachhinein zu erwerben, wenn z. B. eine geschützte Datei zwischen den Nutzern weitergegeben wird und der Sender zwar im

Besitz einer Lizenz ist, diese aber an den Nutzer gebunden ist und nicht weitergegeben wird. [10]

Microsoft Windows Media DRM bietet laut Hersteller u. a. die Vorteile, dass ein Player mit dem Hostcomputer verknüpft wird, wodurch ein Player eindeutig wird. Die Überprüfung bzw. Deaktiverung einzelner ‚gefährdeter' Player, die also Sicherheitslücken beinhalten, mit denen der Datenstrom weiterverwendet werden kann, ist möglich. Ebenso ist es unter Windows XP möglich, den ‚Weg' vom Player zum Soundkartentreiber zu sichern („Secure Audio Path") um ebenfalls nicht autorisierten Programmen den Zugriff zu untersagen.
Ebenso bietet das System die Möglichkeit, Streaming-Daten in Echtzeit zu kodieren.

Zu den größeren Unternehmen, die Windows Media DRM zum Verschlüsseln ihrer Daten einsetzen oder diese wiedergeben können, gehören unter anderem:

- America Online (AOL) & The Disney Co.
- BMG, EMI, Sony, Warner, Universal
- Napster, Musicload.de
- iRiver, Archos, Motorola, Nokia (sowie andere Hersteller von tragbaren Abspielgeräten)
- Real Jukebox, WinAMP, …

Mobile Endgeräte, die den Anforderungen genügen, um mit Windows Media DRM verschlüsselte Daten wiederzugeben, können das von Microsoft vergebene Logo „PlaysForSure" erhalten. Dies erfordert, dass sie kompatibel zu der verwendeten Verschlüsselung sind sowie die erforderlichen Codecs verwenden, um den Inhalt darstellen zu können.

---

[10] Siehe dazu http://www.microsoft.com/windows/windowsmedia/forpros/drm/tutorial.aspx
Beispielfilme zu den Client-Server-Abläufen beim Abspielvorgang
Keywords: windows media drm tutorial

3.4.1.2 FairPlay & Apple's iTunes

Mit der Veröffentlichung der tragbaren Abspielgeräte der iPod-Familie wurden von Apple ebenso die kostenlose Software iTunes angeboten und der iTunes Store (vormals iTunes Music Store) eröffnet. Der iTunes Store bietet Musik und mittlerweile auch Videos zum Kauf und Download an. Diese Daten sind mit dem DRM System FairPlay verschlüsselt. Diese Entwicklung von Apple benutzt verschlüsselte AAC Dateien (Advanced Audio Coding, auf MPEG-2 Part 7 bzw. MPEG-4 Part 3 basierend), die als Weiterentwicklung von MP3 gesehen werden.

Mit dem Konzept, FairPlay-geschützte Dateien nur per iTunes erwerben zu können und auch nur per iTunes auf ausschließlich iPods kopieren zu können, hat Apple ein geschlossenes System geschaffen. Der Zugriff auf den iTunes Store ist mit anderen Anwendungen nicht möglich, ebenso soll der direkte Zugriff auf den iPod nur per iTunes möglich sein (auch wenn es Möglichkeiten gibt, dies zu umgehen).

In der momentanen Lizenzhandhabung (Dezember 2006) ist es möglich, geschützte Musik auf beliebige viele iPods zu kopieren, auf bis zu fünf Computern abzuspielen und beliebig oft auf CD zu brennen.

Der iPod selbst unterstützt ebenfalls keine anderen DRM-Systeme als FairPlay, Windows Media DRM Dateien können somit nicht abgespielt werden. Auch war es für Anbieter von Inhalten bislang nur möglich, die Daten direkt über Apple schützen zu lassen, um sie für den iPod anbieten zu können. FairPlay ist somit nicht – wie z. B. Windows Media DRM – für Firmen als eigenständige Lösung zu erwerben.

3.4.1.3 Helix DRM – RealNetworks

Mit Helix DRM bieten RealNetworks ein DRM System an, das möglichst viele Audio-/Musik-Formate unterstützen soll und die Inkompatibilitäten mit den Endgeräten einschränken soll. Voraussetzung dafür ist die mittlerweile auch unter GPL veröffentlichte Plattform „Helix DNA", die aus Client, Server und Producer (zum kodieren der Daten) besteht.

Der RealPlayer, als kommerzielle Version des Helix Players, ist Voraussetzung für den Zugriff auf den von RealNetworks betriebenen Online Shop Rhapsody (www.rhapsody.com), der mit Helix DRM geschützte Musikstücke anbietet. Dabei können die Stücke entweder gekauft und herunter geladen werden, oder über Streaming direkt angehört werden.

Mit der erstmals im Juli 2004 veröffentlichten Software „Harmony" hat RealNetworks für Aufregung gesorgt, nachdem es durch Reverse-Engineering von Apple's FairPlay möglich war, Helix DRM kodierte Daten in iPod-kompatible FairPlay Daten zu verwandeln und somit als erster nicht von Apple zertifizierter Anbieter DRM-geschützte Daten für den iPod zu vertreiben und dort abzuspielen. Es entwickelten sich sowohl ein Rechtsstreit sowie ein technischer Wettlauf, bei dem Apple versuchte, mit Updates ihrer Software die Kompatibilität der RealNetworks-Lösung zu beenden.

Nach einigen gegenseitigen Updates und einer gescheiterten Petition von Seiten RealNetworks', FairPlay für andere Anbieter zu öffnen, hat sich die Lage entspannt. Heute wirbt Rhapsody weiterhin damit, dass gekaufte Daten noch auf die iPods kopiert werden können. Der neuere Abonnementservice, „Rhapsody To Go" sei aber nicht mit den iPods kompatibel.

3.4.1.4 Adobe DRM

Adobe hat in seinem Portable Document Format (PDF) auch die Möglichkeit integriert, die erstellten PDF-Dokumente per Adobe DRM zu schützen. Wie bei Audio- und Video-Dateien ist der Inhalt verschlüsselt und kann nur gelesen werden, wenn die darstellende Applikation – hier der Adobe Reader ab Version 6.0, früher Acrobat eBook Reader – die Berechtigung zur Anzeige erlangt hat. Von Seiten des Adobe DRM Systems müssen Geräte (wie PCs, MAC, PDAs) zur Darstellung der geschützten PDF-Dateien aktiviert werden, d.h. mit einer Benutzerkennung verknüpft werden, über die dann z. B. Bücher verschiedener Autoren als eBooks erworben werden können.

Zu den Möglichkeiten der Beschränkung, die Adobe DRM bietet, gehört z. B. der Schutz eines Dokumentes, der davor schützt, dass Text kopiert werden kann. Auf Wunsch kann auch die Druckmöglichkeit deaktiviert werden.

Dateien mit einem Ablaufdatum zu versehen ermöglicht dem Anbieter der Bücher, ein Leihsystem wie in einer herkömmlichen Bibliothek zu etablieren und dem Benutzer nur für eine begrenzte Zeit den Zugriff auf die Dateien zu ermöglichen.

3.4.2 Einsatz in Unternehmen

Der Einsatz von DRM-Systemen in Unternehmen, so genanntes Enterprise DRM (E-DRM, ERM) zielt weniger darauf ab, den Zugang zu urheberrechtlich geschützten Daten zu kontrollieren, sondern Betriebsgeheimnisse oder interne Firmendokumente zu schützen. Der bestehende Schutz von Daten auf der Basis von Zugriffsrechten auf Dateiebene reicht heute meist nicht mehr aus. Die Daten sind zwar gegen einen direkten Zugriff geschützt – sollten sie aber mutwillig oder versehentlich von einer zugriffsberechtigten Person weitergeleitet werden, ist keine weitere Kontrolle möglich.

Daten, die per DRM geschützt sind, können dieses Problem lösen. So wäre es zwar möglich, eine Datei mit Betriebsinterna weiterzuleiten, der Empfänger bekäme aber auch hier nur verschlüsselte Daten. Um die Daten zu nutzen, müsste er sich an der entsprechenden Autorisierungsstelle anmelden und bekäme erst dann die Daten zur Verwendung. Sollte die darstellende Applikation dies einschränken, so wäre hier evtl. z. B. eine Kopie des Textes nicht möglich.

Auch die zeitlich begrenzte Gültigkeit von Dokumenten kann hier einerseits von Nutzen sein, um evtl. veraltete Versionen zentral zu deaktivieren und auf neuere Daten hinzuweisen.

Andererseits kann im geschäftlichen Bereich die gesetzliche Regelung zur Aufbewahrungspflicht (z. B. nach § 257 HGB) von Dokumenten auch im Widerspruch zu DRM-Systemen stehen. Entweder müssen die Dokumente somit auf Dauer ungeschützt archiviert werden, oder es muss sichergestellt werden, dass die DRM System auch während der Frist noch funktionstüchtig sind.

Anbieter dieser Systeme gibt es einige, darunter auch Microsoft mit den „Windows Rights Management Services“, „Liquid Machines“, „EDRM Solutions“ und viele andere.

Weiterführende Quellen zum Thema:

Keywords: enterprise digital rights management

4 Kritik an DRM und Trusted Computing

Wer sich mit DRM beschäftigt und eine Suche danach im Internet startet, trifft (abgesehen von weiteren Bedeutungen wie z. B. Digital Radio Mondiale) unweigerlich nicht nur auf Seiten von Anbietern, die Systeme zu diesem Thema vertreiben, sondern verstärkt auch auf Kritik am DRM Konzept. Gerade im Bereich der Film- und insbesondere der Musikindustrie, wie DRM-Systeme am häufigsten eingesetzt werden, gibt es eine Vielzahl an Meinungen zu dem Thema.

Ebenso führt eine Suche nach dem Thema Trusted Computing kaum an der Verbindung von Trusted Computing mit DRM vorbei. Sehr viele Kritiker bzw. Webseiten beschäftigen sich mit der befürchteten Verbindung von Trusted Computing mit DRM und der möglichen negativen Folgen für die Benutzer, was sehr häufig auch als Hauptziel und Zweck der TCG bzw. vormals TCPA genannt wird.

Die meisten Artikel, auf die man bei einer einfachen Suche nach diesen Themen stößt, stammen aus den Jahren 2002 bis 2003. In dieser Zeit wurden die ersten Ergebnisse bzw. Spezifikationen der TCG bekannt gegeben. Dies löste förmlich ein Negativ-Hype unter der Berücksichtigung von Trusted Computing und DRM bis hin zu Verschwörungstheorien aus, dem sich offensichtlich kaum ein Autor entziehen konnte.

Leider finden sich in diesen Artikeln kaum Hinweise darauf, wie genau die Befürchtungen und Einschränkungen der User technisch aussehen sollen. Daher war es für mich eine Grundvoraussetzung bei der Analyse des Themas, in notwendigem Maße auf die technischen Details von Trusted Computing und DRM einzugehen.

Die Kritik an dem Konzept des Trusted Computing bezieht sich hauptsächlich auf die Verbindung mit DRM und die damit verbundenen Möglichkeiten, DRM an sich effizienter durchzusetzen. Allerdings gibt es auch Kritikpunkte an DRM, die sich nicht auf das Zusammenspiel mit Trusted Computing beziehen. Die aufgeführten Punkte

beziehen sich so bereits auf heutige Systeme und sind nicht notwendigerweise in Verbindung mit Trusted Computing zu bringen.

4.1 Kritik an DRM

4.1.1 Generelle Kritik

DRM System bringen in vielen Bereichen Einschränkungen für den Benutzer und werden daher von Kritikern auch als „Digital Restrictions Management" bezeichnet. Die Eingrenzung der verwendeten Hardwaregeräte, der Software für die Wiedergabe bzw. Nutzung und die fehlenden Möglichkeiten, mit Inhalten in gewohnter Art und weise umzugehen, senken die Benutzerfreundlichkeit herab. Dies ist teilweise erwünscht, um die Vervielfältigung der Daten zu verhindern, für den Benutzer bedeutet dies jedoch massive Einschränkungen.

4.1.2 Privatsphäre

Die Wahrung der Privatsphäre von Benutzern bekommt im Zusammenhang mit einigen DRM-Systemen eine neue Komplexität. Weniger bei Offline-DRM-Systemen als bei solchen, die mit einem Server kommunizieren, ist diese Problematik festzustellen. Versuchen einige Systeme, vor der Darstellung eines geschützten Inhaltes die Gültigkeit der Lizenz überprüfen, greifen sie oftmals zwar auf eine etwaige vorher angelegt Kopie der Lizenz zu, sind aber meistens auch darauf angewiesen, mit einer Lizenzierungsstelle zu kommunizieren. Somit ist es erforderlich, für z. B. jedes Musikstück mit einem Server Verbindung aufzunehmen und die Lizenz zu erhalten bzw. zu bestätigen. Bei diesem Vorgang sind für die Überprüfung die genauen Daten des Musikstückes als auch des Benutzers notwendig, um die Lizenz zu verifizieren.

Aus diesen Daten ließen sich detaillierte Nutzungsstatistiken nicht nur über die Musikstücke, sonder auch die Nutzer erstellen. Dies gilt in dieser Form nicht nur für entsprechende Musikangebote, sonder kann auf alle gängigen Pay-per-View Systeme auch im Film- oder eBook-Bereich angewandt werden.

Kritiker dieser Systeme fordern hier also berechtigterweise, dass es vom System gewährleistet werden muss, dass diese Daten – die unzweifelhaft erforderlich sind –

nicht ausgewertet und archiviert werden, außer für den etwaigen Zweck der Abrechnung bei Pauschalmodellen. Es ist also auf der rechtlichen Ebene notwendig, diese Systeme gegen Missbrauch zu schützen und den Schutz der Privatsphäre zu wahren.

Interessant ist in diesem Zusammenhang auch die Tatsache, dass das Thema „Privatsphäre des Nutzers" in Stefiks Artikel und seinen aufgezeigten Szenarien nicht erwähnt wird – eine einfache, technische Lösung scheint hier nicht greifbar.

4.1.3 Beständigkeit

Daten, die mit einem DRM System verschlüsselt werden, sind ohne die entsprechende Berechtigung nicht zugänglich. Einige dieser Systeme setzen voraus, dass die Lizenz vor jedem Zugriff überprüft und dabei auf einen zentralen Lizenzierungsmechanismus zugegriffen werden muss. Dies stellt an den Lizenzgeber einerseits den Anspruch, dass die dafür zuständigen Server jederzeit verfügbar sind, da die Daten sonst nicht entschlüsselt werden können.

Andererseits setzt dies, gerade auch bei längerfristiger Verwendung der Daten, voraus, dass der entsprechende Anbieter noch existiert und somit Lizenzen noch vergibt. Sollte ein Benutzer über einen Anbieter heute z. B. einen Musiktitel erwerben, so muss gewährleistet sein, dass auch Jahre später die Verwendung der Daten noch möglich ist und dementsprechend der Anbieter bzw. dessen Lizenzierungsserver noch in Betrieb ist.

4.1.4 DRM und Beweispflicht von Dokumenten

Hauptsächlich im geschäftlichen Einsatz von DRM-Systemen ist es notwendig, Dokumente auch nach vielen Jahren noch korrekt darstellen zu können. Die gesetzliche Vorhaltepflicht für Dokumente erfordert, dass die Daten, die mit einem DRM System verschlüsselt wurden, auch nach 10 Jahren noch lesbar gemacht werden können. Da es eventuelle nicht sichergestellt ist, dass 10 Jahre später noch der gleiche Lizenzierungsmechanismus verwendet wird bzw. es auch zu Problemen mit der Gewährung von Zugriffsrechten auf Benutzerebene kommen kann, wenn ein Benutzer das Unternehmen verlassen hat. Daher muss vom System bzw. den

Sicherungsprozessen im Unternehmen sichergestellt werden, dass die Daten entweder ggf. unverschlüsselt abgelegt werden, oder es muss sichergestellt werden, dass die DRM-Infrastruktur weiterhin besteht und die Lizenzen auch später wieder vergeben werden können.

4.1.5 Weiterverkauf von Ware

Rechtlich strittig ist der Punkt, wie es mit dem Weiterverkauf von DRM-geschütztem Inhalt aussieht. Erwirbt ein Nutzer eine CD oder DVD, so ist es möglich, diese – als Datenträger mit dem darauf befindlichen urheberrechtlich geschützten Inhalt – im Original jederzeit weiterzuverkaufen. Bei digitaler Musik, die zwar erworben wird, aber keinen materiellen Gegenstand darstellt, wird dies schwierig. Heutige DRM-Systeme lassen diesen Anwendungsfall bisher nicht zu, da kein Benutzer den Zugriff auf ein Musikstück an einen anderen weitergeben kann – schon gar nicht, wenn dieser ein anderes Endgerät besitzt.

(vgl. http://www.netzwelt.de/news/74371_99-musik-weiterverkaufen-erlaubt-vs-verboten.html)

Keywords: drm weiterverkauf ware

4.1.6 Mobilität und Kompatibilität

DRM-Systeme, die zur Überprüfung von Lizenzen eine Verbindung ins Internet benötigen, können in dieser Form häufig nicht für mobile Endgeräte eingesetzt werden. Diese sind nicht in der Lage, die Lizenz online zu überprüfen bzw. zu erlangen, sondern die meisten Lösungen basieren darauf, dass die Lizenz an das Endgerät gebunden wird (vgl. 3.3.3 DRM im mobilen Bereich). Dadurch ist es notwendig, dass die Musikstücke nicht ‚einfach' auf das Gerät kopiert werden, sondern mit der dafür vom DRM System vorgesehenen Software überspielt werden, welche die notwendigen Anpassungen vornimmt.

Allerdings ist es hierbei erforderlich, dass das entsprechende Endgerät das verwendete DRM System unterstützt. Da es hier keine einheitlichen Standards gibt, kann es zu Inkompatibilität kommen. So unterstützt der iPod wie bereits erwähnt keine anderen DRM-Systeme, Windows Media DRM kompatible Systeme können evtl. keine Helix DRM Dateien abspielen usw.

Lediglich nicht geschützte MP3s werden von allen MP3-Playern gleichermaßen abgespielt. So ist es von einem Nutzerstandpunkt aus eher hinderlich, geschützte Musikdateien erworben zu haben, wenn sich diese auf dem ein oder anderen Gerät nicht abspielen lassen.

Eine weitere Problematik ergibt sich aus der Tatsache, dass es unterschiedliche DRM-Systeme gibt, die nicht miteinander kompatibel sind. Wechselt ein Benutzer von einem Endgerät zum anderen, also z. B. von einem iPod von Apple zu einem anderen MP3-Player, der Windows Media DRM Inhalte abspielen kann, so führt dies zum Verlust der Möglichkeit, die Daten auszutauschen. Es wäre somit notwendig, dass der Benutzer einen Musiktitel, den er z. B. bei iTunes erworben hat, erneut bezahlen muss, wenn er ihn bei einem anderen Anbieter für sein neues Gerät beziehen möchte.

Dieser Missstand, also der Kontrollverlust darüber, wo ein Benutzer seine legal erworbenen Titel abspielen kann – gepaart mit der Notwendigkeit, einen Titel mehrmals für verschiedene Geräte erwerben zu müssen – ist einer der Hauptkritikpunkte an gängigen DRM-Systemen. Hier wird auch von einer „Konsumleitplanke" gesprochen, da sich der Konsument mit dem Erwerb eines Endgerätes nicht nur für die Funktionalitäten des Gerätes, sondern auch gleichzeitig für mögliche Anbieter von Inhalten entscheiden muss.

4.1.7 Umzug von Geräten

Viele DRM-Systeme verwenden zur Bindung der Daten an einen Nutzer eine ID, welche das Endgerät (mobil oder nicht) identifiziert. So wird sichergestellt, dass die Datei – wenn die Lizenz dies erfordert – nicht von beliebig vielen Geräten evtl. auch anderer Anwender abgespielt werden kann. Wird somit z. B. eine neue Lizenz für ein Musikstück an einen Anwender ausgegeben und dabei an ein neues System geknüpft, so wird dies verzeichnet. Je nach Lizenz ist es dann evtl. nicht mehr möglich, einen weiteren Rechner zum Abspielen zu verwenden.

Dies führt gezwungenermaßen beim Hardwarewechsel zu Problemen. Sollte sich die entsprechende – von der Hardware bestimmte – ID ändern, so weigert sich der

Player, die Daten abzuspielen – schließlich passt die Lizenz nicht mehr zum angegebenen System.

Technisch ist es bei einigen Systemen vorgesehen, dieses Problem auf verschiedensten Wegen zu umgehen. Bei Apple's iTunes ist es z. B. möglich, von den fünf erlaubten Bindungen (Authorization) eine einzelne Bindung eines Benutzerkontos zum Rechner aufzuheben – was zum Verlust der Möglichkeit führt, mobile Endgeräte von dieser Maschine aus mit Musikstücken zu versorgen oder geschützt Musik abzuspielen. Ohne direkte Bindung lässt sich geschützte Musik von diesem Rechner lediglich noch kopieren, aber nicht mehr direkt nutzen[11].

Andere Systeme gestatten hingegen dem Nutzer, in regelmäßigen Abständen ein neues System an die Lizenzen zu binden. Der Anbieter von zusätzlichen Soundtracks zu Computerspielen DirectSong www.directsong.com gestattet beispielsweise, dass alle 6 Monate ein neues System zusätzlich zu den vier verfügbaren Lizenzen installiert werden kann.

Auch wenn es technische Möglichkeiten gibt, den Umzug auf ein anderes System problemlos zu überstehen, so führen die notwendigen Schritte bei vielen Anwendern zu Verwirrung – oder die Maßnahmen werden einfach vergessen. Sei es durch Neuinstallation nach einem Systemausfall, Austausch von einzelnen Komponenten am System oder vollständigem Wechsel der Hardware, führt es bei vielen Anwendern zu Problemen, wenn die erworbene Musik nicht mehr läuft. Gerade wenn der Nutzer einen Musiktitel erworben hat, anstatt ihn in Internettauschbörsen herunter zu laden, ist es umso ärgerlicher, wenn sich dadurch eher Probleme und Einschränkungen ergeben.

4.2 DRM und die Auswüchse

Dass dem Schutz der rechtlich geschützten Inhalte bei den Produzenten von Musik- und Filminhalten und der Einschränkung der Nutzung ein großes Interesse zukommt,

[11] http://www.apple.com/support/itunes/musicstore/authorization/
Keywords : itunes deauthorize

lässt sich anhand einiger sehr rigoroser Beispiele ersehen. Einzelne Unternehmen gehen dabei so weit, dass sie sich auf rechtlich fragwürdigen Wegen die Sicherung ihrer Interessen erzwingen wollen.

4.2.1 XCP Kopierschutz aka SonyBMG RootKit

Am 31.10.2005 beschreibt der Sicherheitsexperte Mark Russinovich in seinem Blog ein RootKit[12], das sich über eine Audio-CD aus dem Hause Sony BMG installiert hat. Ziel der Software ist, den Zugriff auf das CD-Laufwerk zu verweigern, wenn ein ‚verdächtiges' Programm (z. B. CD-Kopierprogramm) versucht, zuzugreifen. Des Weiteren werden die entsprechenden installieren Treiber vor dem Benutzer versteckt.

Dieser ersten Meldung folgt in den darauf folgenden Tagen und Wochen ein Sturm an Protesten gegen diesen Kopierschutz. Mehrere Punkte und Pannen im Zusammenhang mit der Software ließen das Vorgehen Sonys als recht zweifelhaft erscheinen. So wurde der Benutzer bei der Installation des notwendigen Players nicht über den vollen Umfang der Software informiert. Außerdem versteckt die Software nicht nur ‚eigene' Dateien, sondern ist auch in der Lage, beliebige Dateien anderer Programme zu verbergen. So erfährt das RootKit recht schnell großer Beliebtheit bei Programmieren von Trojanern und Würmern. Später wurde auch festgestellt, dass die Software Verbindung zu Sony-eigenen Servern aufnimmt und Nutzungsdaten übermittelt. Um so größer die Empörung, als auch noch festgestellt wird, dass die Software auch Teile von Programmen enthält, die unter der freien Lizenz GPL verwendet werden dürfen – was in diesem Fall aber einer Kopierrechtsverletzung gleichkommt.

Nachdem man bei Sony festgestellt hat, welcher Aufschrei sich von der Community der Sicherheitsexperten im Internet bis hin zu großen Nachrichtenagenturen entwickelt hat, versuchte man, den Schaden zu begrenzen. Es wurde ein „Uninstaller"

---

[12] RootKit: ursprünglich in der Unix-Welt eine Programmsammlung, die im System läuft und verhindern soll, dass der Administrator (root) erkennen kann, dass sich andere Personen mit Administrator-Rechten anmelden können. Dabei werden z. B. Dateien oder Verzeichnisse versteckt, Logfiles geändert oder Hintertüren in das System geöffnet.
Heute auch auf Nicht-Unix-Plattformen verwendeter Begriff.

angeboten, der das System entfernen sollte – aber dabei eine weitere Sicherheitslücke aufreist.

Die CDs werden vom Markt genommen, während eine Reihe von Sammelklagen gegen Sony gestartet werden, Sony CDs an manchen Arbeitsplätzen verboten und aus Bibliotheken genommen werden.

Quellen:

http://netzpolitik.org/2005/rookit-sonys-digitaler-hausfriedensbruch/

http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

Keywords: sony rootkit

4.2.2 Weitere zweifelhafte Kopierschutz-Mechanismen

Nicht nur für Audio-CDs, auch für DVDs existieren vermeintlich notwendige Kopierschutzprogramme. So existiert z. B. für die DVD „Mr & Mrs Smith" aus dem Kinowelt-Verleih der Kopierschutzmechanismus Alpha-DVD von Settec. Auf einigen Systemen verursacht dieser Treiber Instabilitäten, führt zu Fehlern beim Brennen von anderen DVDs und lässt sich auch nur unter hohem Aufwand wieder entfernen (vgl. http://www.heise.de/newsticker/meldung/69211). Dies erscheint für den User umso ‚unnötig ärgerlicher', da der installierte Treiber offensichtlich erstens keinen wirklichen Schutz der DVD vor Kopierversuchen bietet und sich zweitens die DVD auch abspielen lässt, wenn die Autostart-Funktion des Laufwerkes deaktiviert wird.

Weniger freundlich verhält sich ein weiteres Kopierschutz-System aus dem Hause Sony. „MediaMax" geht so weit, sogar bevor der User den Lizenzvertrag aktiviert, Zusatzsoftware zu installieren. Sogar wenn der Benutzer den Lizenzvertrag ablehnt, bleibt die Software auf dem System installiert und aktiviert sich evtl. sogar selbst. (vgl. http://www.freedom-to-tinker.com/?p=936). Bedenklich auch hier, dass die Software statistische Daten über die gespielten Titel an Server von Sony BMG schickt, ohne dass der User hier die Möglichkeit hat, dies abzulehnen.

4.3 DRM und die Wege daran vorbei

Seitdem es DRM-Systeme gibt, es also manchem Nutzer nicht mehr möglich ist, bestimmte Daten wie gewohnt zu vervielfältigen oder zu portieren, wird versucht, diese Systeme zu umgehen. Nicht nur der Drang von Hackern, die Systeme auszuhebeln – sei es wegen des ‚sportlichen Ehrgeizes' eines Hackers oder um die ehemals geschützten Daten wieder vervielfältigen zu können – sondern auch wirtschaftliche Interessen von Firmen können die Umgehung des Inhaltsschutzes vorantreiben.

4.3.1 Jon Lech Johansen vs. CSS

Der 1996 entwickelte und in allen DVD-Playern implementierte symmetrische Verschlüsselungsalgorithmus CSS wurde im Oktober 1999 von mehreren Crackergruppen gebrochen. Seit dem wird das Programm DeCSS verwendet, um den – ob schon durch Designfehler oder damalige Exportbestimmungen – sehr schwachen Verschlüsselungscode einer DVD zu errechnen.

Das Verfahren wurde über „Reverse Engineering" gebrochen und die Berechnungen zur Umgehung des Schlüssels wurden nach Bekanntwerden der ersten Entschlüsselungsmethoden weiter verfeinert.

Auch wenn es sich um mehrere Gruppen und auch mehrere Personen handelte, die das Verfahren umgingen, wurde der damals 15jährige Norweger Jon Lech Johansen verhaftet und verklagt. Es kam im folgenden Gerichtsverfahren in erster und zweiter Instanz allerdings zu einem Freispruch, da das Kopieren von DVD-Filmen nicht als illegal betrachtet wurde.

Quellen:

http://de.wikipedia.org/ und - Artikel „Content Scrambling System" (Stand 11:22, 24. Dez. 2006) sowie „DeCSS" (Stand 04:27, 9. Dez. 2006) sowie http://en.wikipedia.org/

4.3.2 Real vs. Apple

RealNetworks hatten sich im Juli 2004 mit „Harmony“ die Möglichkeit eröffnet, über den RealPlayer von Real geschützte Musik auf den iPod zu kopieren (vgl. 3.4.1.3 Helix DRM – RealNetworks) und für ihre Kunden anzubieten.

Offensichtlich war es hier nicht nur für ‚Hacker’ interessant, rechtlich fragwürdige Techniken wie Reverse Engineering einzusetzen, um einen DRM-Mechanismus zu umgehen. Das technische Wettrüsten der Versionen von Apple und Real (neue Verschlüsselung seitens Apple, daraufhin neue Version von „Harmony“) wurde begleitet von rechtlichen Verhandlungen.

4.3.3 Jon Lech Johansen vs. Apple

Nachdem er damals CSS per Reverse Engineering umgangen hatte, entwickelte er in den letzten Jahren immer wieder Programme wie PlayFair und DeDRMS, um FairPlay von Apple zu umgehen.

Im Oktober 2006 konnte Jon Lech Johansen verkünden[13], dass er auch das FairPlay System von Apple für andere öffnen könne. Hierbei ging es nicht darum, die geschützten Dateien zu entschlüsseln, sondern selbst Dateien per FairPlay verschlüsseln zu können, so dass sie auf iPods durchaus DRM-geschützt ablaufen können. Bisher war dies für Musikanbieter nur mit Lizenzierung von Apple möglich.

Mit dieser Software und seiner Firma DoubleTwist Ventures kann Johansen nun anderen Musikanbietern ermöglichen, dass sie ihre Musikstücke nun ebenfalls für den iPod anbieten können, ohne dass sie über Apple’s iTunes erworben werden

4.3.4 FairUse4WM vs. Microsoft

Im August 2006 tauchte ein Programm namens FairUse4WM von einem unbekannten Autor mit dem Pseudonym „viodentia“ in einem Forum[14]im Internet auf.

---

[13] http://www.heise.de/newsticker/meldung/78974

Keywords: johansen fairplay

[14] http://forum.doom9.org/showthread.php?t=114916

Keywords: fairuse4wm

Dieses Programm war in der Lage, Windows Media DRM Dateien ihrer Verschlüsselung zu entledigen. Voraussetzung dafür war, dass der Benutzer tatsächlich im Besitz der entsprechenden Lizenz war – es konnten also nicht beliebige Dateien entschlüsselt werden sondern lediglich jene, deren Verwendung dem Nutzer zu diesem Zeitpunkt tatsächlich gestattet war. Somit war es allerdings möglich, über zeitliche begrenzte Probe- oder Gratisangebote Dateien zu beziehen, diese frei zu schalten und nach Ablauf der Testphase weiter zu verwenden.

Microsoft stellte daraufhin ein Update der internen Funktionen ihres DRM-Systems zu Verfügung, um FairUse4WM zu deaktivieren – kurze Zeit darauf erschien allerdings ein Update der unerwünschten Software, das diese Änderungen erneut umgehen konnte.

Heute existiert FairUse4WM in Version 1.3 und scheint in der Lage zu sein, auch aktuelle Windows Media DRM-Systeme umgehen zu können. Im Moment sind rechtliche Schritte gegen den Hacker Viodentia eingeleitet, dessen Identität anscheinend noch ungeklärt ist und Betreiber von Webseiten, die das Programm hosten, werden von Microsoft abgemahnt.

4.3.5 Dmitry Sklyarov vs. Adobe

Der Russe Dmitry Sklyarov wurde im Jahr 2001 in den USA verhaftet, da er ein Programm zur Umgehung des Schutzes von Adobe eBooks geschrieben hatte. Der Fall erhielt unter anderem deswegen starke Aufmerksamkeit, da das Programm in Russland nicht illegal war, wohl aber gegen den Digital Millennium Copyright Act (DMCA) der Vereinigten Staaten verstieß. Er sowie die Firma Elcomsoft, die das Produkt vertrieb, wurden allerdings kurz darauf frei gesprochen.

4.3.6 Die „analoge Lücke“

Eine stets existierende Möglichkeit, geschützten Inhalt anderweitig zu verwenden, entsteht durch die sog. „analoge Lücke“. Damit werden die Möglichkeiten bezeichnet, Musik aus einem Lautsprecher eben mit einem Mikrofon aufnehmen zu können, Filme mit einer Kamera abfilmen zu können oder auch Text abfotografieren

oder gar abschreiben zu können – und damit digitale Daten wieder digital aufzeichnen zu können.

Nach diesem Prinzip arbeitet auch Tunebite[15], ein Programm zur Verwandlung DRM-geschützter Dateien in freie. Über eine virtuelle Soundkarte werden hierbei Daten in ein pseudo-analoges Signal verwandelt, dass gleichzeitig wieder aufgenommen wird, dabei allerdings den Rechner nicht verlässt. Da ein analoges Kopieren von Daten erlaubt ist und die Daten neu kodiert werden (also eventuell verlustbehaftet verfahren wird), verstößt diese Vorgehensweise nicht gegen geltendes Recht.

Da es gegen diese Verfahren kaum eine Möglichkeit gibt, versuchen einige Hersteller, ihre Werke mit (digitalen) Wasserzeichen zu versehen, um zwar die Weiterverwendung nicht schützen, aber evtl. zurückverfolgen zu können, wo ein Werk entschlüsselt bzw. reproduziert wurde.

4.4 Kritik an den Spezifikationen der TCG

Die Kritik an den Spezifikationen der TCG, die sich seit mehreren Jahren kaum verändert hat, bezieht sich hauptsächlich auf einen Aspekt: Die Möglichkeit, Systeme mit einem TPM und einer darauf basierenden Hard- und Softwarearchitektur überwachen bzw. überprüfen zu können. Per „Remote Attestation“ (2.2.2.3 Beglaubigung (Remote Attestation)) kann sichergestellt werden, dass ein System nur dann mit einer Gegenstelle in Interaktion treten darf, wenn es eine genau vorgeschriebene Konfiguration hat. Dies erleichtert die Durchsetzung von DRM-Beschränkungen.

Weitere Kritikpunkte werden in Auseinandersetzungen mit dem Thema Trusted Computing im Internet kaum sichtbar, sollen hier jedoch kurz aufgeführt werden. Weiterhin existiert auch kaum ein Artikel, der sich mit der Arbeit der verschiedenen Arbeitsgruppen auseinandersetzt.

[15] http://www.tunebite.de/

4.4.1 Technische Kritik

Rüdiger Weiß, Kryptograph, Mathematiker und TCG-Kritiker stellt in seinem Vortrag „Hashing Trusted Computing“[16], gehalten auf dem 22. Chaos Communication Congress des Chaos Computer Clubs im Dezember 2005 fest, dass die Spezifikation teilweise auf gebrochenen Algorithmen beruht. In der Spezifikation festegelegte Mechanismen (z. B. SHA-1 und darauf aufbauende Verschlüsselungsmethoden) können vom kryptographischen Standpunkt aus als gebrochen betrachtet werden, auch wenn die Folgen bisher noch nicht schwerwiegend sind. (vgl. www.schneier.com, Weblog von Bruce Schneier, Artikel vom 18. Februar 200517) Weitere Angriffe und Verbesserungen des kryptographischen Wissens über Hash-Algorithmen werden erwartet und so empfiehlt Weiß die Verwendung komplexerer Algorithmen.

4.4.2 Konzeptionelle Kritik

Die verbreitete Kritik an „Trusted Computing“ bezieht sich hauptsächlich weniger auf die Arbeit der Trusted Computing Group und deren verschiedene Arbeitsgruppen, sondern es reduziert sich auf den Punkt der Remote Attestation (2.2.2.3 Beglaubigung (Remote Attestation)). Hierbei wird davon ausgegangen, dass Remote Attestation eingesetzt wird, um dem Benutzer die Konfiguration und Umgebung vorzuschreiben, die verwendet werden soll um (DRM-geschützte) Musik oder Filme abzuspielen oder andere vergleichbare Anwendungen zu benutzen.

Diese Kritik geht hauptsächlich in Richtung aller Szenarien, in denen es aus Sicht des Anwenders wünschenswert ist, dass er selbst bestimmen kann, welche Software er nutzt. Die Wahl der Software könnte mit „Remote Attestation“ eingeschränkt werden, wenn es um den Zugriff auf Daten geht. Kann sich ein Samba-Server heute wie ein Windows File Server verhalten und sich ein Firefox als ein anderer Browser ausgeben, so könnte dies durch „Remote Attestation“ unterbunden werden – denn die Komponenten eines Systems können eindeutig identifiziert werden.

---

[16] http://events.ccc.de/congress/2005/fahrplan/events/495.en.html

[17] http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

Zusammen mit der Funktion des Sealing (2.2.2.1 Versiegelung (Sealing)) ist es dabei zusätzlich möglich, dass Applikationen auf einem Client Daten so verschlüsseln, dass keine andere Anwendung auf diese zugreifen kann.

Die Verwendung dieser Möglichkeiten ist vielfältig. Im Online Banking Bereich lässt sich hierbei möglicherweise die Sicherheit der Transaktionen erhöhen. Eine unerwünschte Änderung der Systemkonfiguration durch einen Virus oder sonstige Schadsoftware könnte so erkannt werden – genauso kann dies aber auch zur Durchsetzung von DRM oder Unterstützung von Monopolen verwendet werden.

Um dies zu unterbinden, fordert die Electronic Frontier Foundation (EFF) einen Mechanismus, den sie „Owner Override" nennen. Die Idee ist, dass nicht ein Dienstanbieter festlegt, wann und in welcher Konfiguration ein System „sicher" bzw. „trusted" ist und die Attestation erfolgreich ist, sondern dass der Benutzer am System selbst festlegt, wann dies der Fall ist. Er stellt seinen gewünschten Systemzustand her und bestimmt diesen als „trusted". Somit kann weiterhin festgestellt werden, ob ein System unerwünschterweise geändert wurde. Der Systemzustand wird nicht von außerhalb vorgeschrieben.

Die TCG lehnt diese Vorgehensweise ab. In einem Interview mit golem.de sagte Thorsten Stremlau, ThinkVantage Consultant bei IBM[18]:

> **Stremlau:** Der Owner hat die freie Wahl, ob das TPM überhaupt aktiviert wird. Die Spezifikationen der TCG sehen keinen Owner Override im von der EFF beschriebenen Sinne vor, da dieser Owner Override negative Konsequenzen für den Endanwender hat. Die Überprüfung eines Bankrechners wäre zum Beispiel nicht mehr möglich und der Benutzer müsste wieder auf blindes Vertrauen zurückgreifen. Dementsprechend ist die Frage des Owner Override kein Diskussionspunkt in der TCG.
>
> **Golem.de:** Welche negativen Konsequenzen könnten dies konkret sein? Inwiefern wäre die Überprüfung eines Bankrechners nicht mehr möglich?
>
> **Stremlau:** Ein Owner Override könnte der Bank ermöglichen, ein fehlerhaftes System als korrekt zu attestieren. Somit kann ein Benutzer

[18] http://www.golem.de/0312/28464.html

während der Transaktion nicht sicher feststellen, ob die Bank wirklich korrekt ist oder ob sie den Owner Override verwendet hat.

Angesichts dessen, dass die Kritik der EFF aus der Sicht der User kommt, geht diese Argumentation offensichtlich in die falsche Richtung. Ein User wird per se stets davon ausgehen müssen, dass ein Bankrechner sicher zu sein hat. Es scheint nicht offen ausgesprochen zu werden, dass das Misstrauen in der Spezifikation eher gegen den Anwender gerichtet ist und dieser nicht die Möglichkeit des Owner Overrides bekommen soll.

In ähnlicher Weise wie der geforderte Owner Override der EFF hat der Chaos Computer Club bereits im März 2003 Forderungen an die IBM überreicht, die aus Sicht des CCC erfüllt werden müssen, um Trusted Computing den Verdacht zu nehmen, dass es sich nur darum drehe, „die kommerziellen Interessen diverser Firmen […] zu schützen“[19]. Die erste Forderung, der User solle die vollständige Kontrolle aller Schlüssel erhalten, wurde von der (damals noch) TCPA allerdings nicht erfüllt. Denn auch mit dieser Kontrolle durch den User würden die Szenarien zur Durchsetzung von DRM verhindert.

Quelle:

http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php

Keywords: eff trusted computing

http://www.heise.de/ct/03/15/021/default.shtml

Keywords: ccc forderungen tcpa

[19] http://www.ccc.de/digital-rights/forderungen

5 Aktuelle Tendenzen

In diesem Kapitel sollen aktuelle Ereignisse betrachtet werden, die sowohl im Zusammenhang mit Trusted Computing als auch mit DRM stehen und diese beiden Themen im Rahmen der Betrachtung dieser Arbeit in Zukunft beeinflussen werden.

5.1 Aktuelle Ereignisse im Bereich DRM

Die dargestellten Informationen beziehen sich meist auf aktuelle Nachrichten vom November und Dezember 2006 und sollen einen Überblick über die Tendenzen im DRM-Markt geben.

5.1.1 Bill Gates, Microsoft und der neue zune

Nicht nur die Benutzer scheinen mit Digital Rights Management unzufrieden zu sein, auch Bill Gates sieht noch Probleme. Bei einem Treffen ausgewählter Blogger[20] habe er gesagt, dass DRM-Systeme noch nicht da seien, wo sie sein sollten. Er wird zitiert mit den Worten: "People should just buy a cd and rip it. You are legal then". [21]

Ob sich dies mit Microsofts gerade in den USA erschienenen und für Ende 2007 in Europa angekündigten tragbaren MP3-Player „zune" ändern wird, bleibt fraglich. Bei diesem Geräte hat Microsoft damit überrascht, dass der erste Microsoft-eigene Player nicht mit Microsoft PlaysForSure kompatibel sein wird. Konkret geht man mit zune dazu über, den Ansatz von Apple mit dem iPod und iTunes zu übernehmen. Der zune kann diverse freie Musikformate abspielen, aber nicht mit Microsofts Windows Media DRM geschützte Inhalte. Stattdessen wird ein eigener Onlineshop, „zune marketplace" (vergleichbar mit iTunes) eröffnet, in dem es nur Inhalte für den neuen Player geben wird. Der bisherige Shop MSN Music wird eingestellt und Benutzern empfohlen, sich einen zune zuzulegen oder zu „Real Rhapsody zu wechseln". Für die Anwender eine weitere Quelle für Missverständnisse, was die (nicht vorhandene) Kompatibilität von DRM-Systemen – in diesem Fall sogar aus dem gleichen Hause – betrifft.

---

[20] http://www.heise.de/newsticker/meldung/82606

[21] http://www.techcrunch.com/2006/12/14/bill-gates-on-the-future-of-drm/

Eine weitere Überraschung bietet der zune auf dem Bereich des Datenaustausches. Mit WLan ausgestattet, bietet der zune die Möglichkeit, Dateien von einem Gerät drahtlos zum anderen zu kopieren. Da man allerdings das eventuell illegale Kopieren von Daten verhindern will, ist der zune mit einer automatischen Einschränkung ausgestattet. Eine auf diesem Wege kopierte Datei kann auf dem Zielgeräte nur für drei Tage bzw. höchstens dreimal angehört werden. Danach müsste der Anwender versuchen, den Inhalt z. B. im zune marketplace zu erwerben. Dies gilt auch, wenn es sich z. B. um einen selbst aufgenommenen Song handelt und genau so für Inhalte, die unter der Creative Commons license[22] verfügbar sind. Diese dabei einem Kopierschutz zu unterwerfen (wenn auch keine Änderung an den Daten vorgenommen wird) sehen einige Kritiker als Bruch der CCL.

Erstaunlich, dass allerdings auch schon eine Umgehung des Schutzes gefunden wurde: Zu kopierende Dateien z. B. von „.mp3" in „.jpg" umbenennen, dann auf das andere Geräte kopieren und dort den Dateinamen wieder korrigieren – schon ist das ausgeklügelte System ausgehebelt[23].

5.1.2 DRM und das Recht auf Privatkopie

Während es in der Schweiz nun offiziell erlaubt ist, DRM-Systeme für den Eigengebrauch zu umgehen[24], läuft seit Juli 2006 eine Offensive des Verbraucherzentrale Bundesverbandes gegen die meisten Anbieter von Musik-Onlineshops.[25] Rechtlich seien die meisten AGBs zweifelhaft und bestehende Rechte werden ignoriert.

---

[22] http://creativecommons.org/

[23] http://www.smorgasbord.net/howto_break_zunes_wifi_drm

Keywords: break zune drm

[24] http://www.handycheats.de/seiten/news/mails/153/1166619005.html

Keywords: schweizer drm eigengebrauch

[25] http://www.vzbv.de/go/presse/749/8/36/index.html

Keywords: vzbv drm rechtloser raum

5.1.3 DRM-freie Alternativen wachsen

Die Anbieter von DRM-freie Musikportalen mehren sich und finden offensichtlich verstärkt Anklang. Dabei handelt es sich nicht nur um Anbieter, die am Rande der Legalität operieren (wie z. B. der russische Betreiber http://allofmp3.com, der fehlende Gesetze in Russland ausnutzt) sowie Anbieter, die auf DRM-freie Inhalte unbekannterer bzw. nicht bei den großen Plattenlabels unter Vertrag stehenden Musikern setzen. Die Liste der Anbieter wächst ebenso wie die Zahl der alternativen Ansätze, was den Vertrieb von Musik betrifft. Bei AmieStreet (http://amiestreet.com/) können alle neu angebotenen Songs kostenlos herunter geladen werden. Der Preis richtet sich dann danach, wie beliebt der Titel ist uns steigt entsprechend.

Auch Yahoo! hat im Juli 2006 einen DRM-freien Song von Jessica Simpson (die bei Epic Records, somit indirekt ausgerechnet bei Sony BMG unter Vertrag steht) angeboten. Der Music Blog von Yahoo[26] weist dabei auch darauf hin, dass DRM nicht im Sinne von Yahoo ist und sie die dafür notwendigen Kosten lieber in andere Dienste stecken. Hierbei wird darauf verwiesen, lieber den Community-Aspekt der Musik zu verstärken und gegenseitige Empfehlungen aussprechen zu können.

Dieser Aspekt, Musik als Community zu sehen wird bei Lastfm.com vertieft. Der auf Streaming basierende Anbieter von personalisierten Webradio-Kanälen ermöglicht den Benutzern, über Plugins in den auch lokal verwendeten Playern wie WinAMP, iTunes oder Windows Media Player, die Liste der gehörten Titel hochzuladen und erstellt daraus Profile, um weitere Musik bekannter und unbekannter Bands zu empfehlen.

Vergleichbar mit einem Musikliebhaber, der mit gedrückter Pause-Taste seines Kassettendecks auf den Wunschtitel im Radio wartet ist der Service von Flatster (http://flatster.com/) vergleichbar. Die Software wartet darauf, dass der gewünschte Titel in einem Webradio läuft und ist dann in der Lage, die digitale Aufnahme zu starten. Interessante Ansätze dieser Art, geltendes Recht umzusetzen um DRM-System zu umgehen, werden wohl auch weiter wachsen.

---

[26] http://ymusicblog.com/blog/2006/07/19/buy-a-customized-jessica-simpson-mp3-at-yahoo-music/

5.1.4 Alternative Flatrate

Vermehrt wird auch die Forderung nach einer allgemeinen Musik Flatrate laut. Unter http://www.Privatkopie.net[27] wird eine Studie veröffentlicht, dass eine Content-Flatrate möglich und nach geltendem Europäischem Recht durchführbar ist. Diese Flatrate könnte den legalen Tausch jeglicher urheberrechtlich geschützter Inhalte unter der Voraussetzung einer monatlichen Abgabe ermöglichen. Eine Entkriminalisierung der nicht mehr aufzuhaltenden Peer-to-Peer-Netzwerke würde dadurch erreicht.

Peter Jenner, der ehemalige Manager von Pink Floyd und weiteren Künstler sowie Generalsekretär des „International Music Managers Forum" sieht laut einem Interview vom November 2006[28] eine Chance, dass in drei Jahren Musik DRM-frei sein wird und eine „blanket license" (vgl. Flatrate) in den meisten Ländern existieren wird.

5.2 Aktuelle Ereignisse im Bereich Trusted Computing

5.2.1 Arbeit der TCG

Die Spezifikationen der TCG werden nur sehr langsam erweitert während bei einigen der Arbeitsgruppen noch keine wirklich konkreten, spezialisierten Spezifikationen vorhanden sind.

Trusted Platform Modules werden verbaut und befinden sich in immer mehr Rechnern, werden dort aber bisher kaum genutzt.

5.2.2 Windows Vista

Wie weit das neu erschienene Windows Vista wirklich weitergehende Unterstützung für TPMs und dazugehörige Szenarien als den bereits beschriebenen Secure Startup (vgl. 2.3.3.1 Microsoft - von Palladium über NGSCB zu BitLocker) liefern kann, bleibt abzusehen.

---

[27] http://www.privatkopie.net/files/PM-060425.html

[28] http://www.theregister.co.uk/2006/11/03/peter_jenner/

Für die Integration von HDTV bietet Windows Vista wohl Unterstützung die auch darauf abzielt, den digitalen Inhalt zu schützen. Es ist aber davon auszugehen, dass die ohnehin schon enthaltenen Funktionen von Windows Media DRM (vgl. 3.4.1.1 Windows Media DRM – PlaysForSure – Microsoft) erweitert werden. Eine Verbindung mit den Vorgaben von Trusted Computing oder gar deren Voraussetzung ist aber noch nicht abzusehen.

Weiterführende Quellen:

http://badvista.org/

http://www.eff.org/IP/fairuse/

http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.txt

http://www.pcstats.com/articleview.cfm?articleID=1871

6 Zusammenfassung

DRM und Trusted Computing – Herr der eigenen Hardware? Als ich mit der Erarbeitung des Themas begann, war ich über die Flut der Panik-artigen Negativ-Meldungen zum Thema TCPA bzw. TCG überrascht. Viele ‚Endzeit-Szenarien der Informationsfreiheit', allen voran die „Trusted Computing FAQ 1.1" von Ross Anderson[29] haben mich zu der Absicht geführt, mit eine objektiven Analyse und einem Überblick über die Spezifikationen der TCG, die Artikel objektiv relativeren zu können. Bestätigt fühlte ich mich in meiner Vermutung, also ich die Webseite „Against TCPA" (http://againsttcpa.com/) mit dem Wahlspruch „It began 2002 and will last as long as needed" mit einem letzten Update vom 05. October 2005 fand.

Die Panik scheint verflogen… Berechtigterweise?

6.1 Fazit

Die Spezifikationen der TCG sind in ihrer vollen Ausprägung und unter Berücksichtigung der Ziele aller verschiedenen Arbeitsgruppen ein mächtiges Werkzeug mit der Möglichkeit, weit in zukünftige Computersysteme eingreifen zu können – was ‚gut' oder ‚böse' genutzt werden kann.

Viele Funktionalitäten können in verschiedensten Anwendungen die (Daten-) Sicherheit für den Benutzer erhöhen, den Administratoren von großen Firmennetzen dienen und im Bereich der Transaktionen im Internet zur Sicherung genutzt werden. So sieht die Spezifikation z. B. auch vor, dass die Sicherheit von Daten im Bereich der Eingabe gewährleistet sein soll, in dem neue Peripheriegeräte den Datenaustausch verbessern und damit z. B. Keylogger ausschließt.

Gerade im Bereich solcher Anwendungen ist von Seiten der Spezifikationen allerdings bisher wenig festgelegt, entsprechende Produkte sind nicht vorhanden. Das TPM wird hingegen bereits verbaut und teilweise verwendet, dieser Teil der

[29] http://moon.hipjoint.de/tcpa-palladium-faq-de.html (de) bzw. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (en)

Spezifikation wurde vergleichsweise schnell realisiert. Die Forderungen von Kritikern und Datenschützern, Trusted Computing die Möglichkeit zum teilweisen Ausschluss des Benutzers aus dem System zu nehmen, wurden allerdings nicht angenommen.

Es bleibt also dabei, dass es der User ist, dem ein „Trusted System" misstraut bzw. misstrauen kann. Wie in dem sehenswerten Kurzfilm „Trusted Computing" (http://www.lafkon.net/tc/) dargestellt wird bleibt die Frage: „If they don't trust you, why should you trust them?"

Selbst das Bundesministerium für Sicherheit in der Informationstechnik sieht im Misstrauen dem Benutzer gegenüber, also dem möglichen Kontrollverlust, denn Sinn eines TPM:

> „Erst auf Grund dieses Mangels an vollständiger Kontrolle durch den Besitzer kann die Vertrauenswürdigkeit der Plattform auch gegenüber Dritten garantiert werden. Somit stellt der Kontrollverlust in gewisser Weise den Hauptnutzen eines TPM dar."[30]

Andererseits macht auch nicht die Hardware allein ver- oder misstrauenswürdiges System aus, sondern das darauf aufbauende Betriebssystem und die Nutzung des technisch Möglichen. Mit Initiativen wie OpenTC (2.3.3.2 OpenTC – Open Trusted Computing) und Turaya (2.3.3.3 Turaya – EMSCB) werden Systeme entwickelt, die das ‚gegenseitige Vertrauen' in den Vordergrund stellen.

Dass „Trusted Computing" ausschließlich zertifizierte Software zulassen wird oder eigene Entwicklungen und OpenSource Anwendungen nicht mehr laufen werden (wie von einigen Kritikern befürchtet), wird so wohl nicht eintreffen können. Es ist utopisch, ein komplettes Betriebssystem als 100% fehlerfrei zu bezeichnen und ihm das volle Vertrauen zu schenken. Somit werden auch in zukünftigen Systemen zwei getrennte Teile laufen – der eine, evtl. kleinere mit den überprüften und sicheren Anwendungen und der andere, in dem bisherige Anwendungen weiterlaufen können.

---

[30] http://www.bsi.de/sichere_plattformen/trustcomp/infos/tpm_report/tpm_grundlagen.htm
Keywords: bsi tpm grundlagen

Es ist momentan nicht vorstellbar, dass ein Betriebssystem rigoros jegliche ‚ungewollte' Software aussperren kann. Sollte dies passieren, dann könnte man es sich als Teil einer Art hersteller- oder dienstanbieterbezogenen Set-Top-Box vorstellen. Sozusagen ein Computer als geschlossene „Sony BMG Box", die vorkonfiguriert und vielleicht sogar einfach vermietet statt verkauft wird. Dafür werden aber wohl eher Spiel- und Multimedia-Konsolen wie Playstation und XBox 360 herhalten.

Ist also der Anwender in Zukunft noch Herr seiner eigenen Hardware? Mit Trusted Computing ist es definitiv technisch möglich, dem Benutzer die Verfügungsgewalt über seine Hardware einzuschränken. Welche Formen diese Einschränkung also annehmen darf, muss auf der rechtlichen Ebene entschieden werden.

Bedenklich ist hierbei, zu sehen, weit einige Anbieter von urheberrechtlich geschützten Inhalten gehen würden um ihre Interessen zu wahren. Dies hat sich im Falle des Sony BMG RootKits gezeigt. Sony musste zwar rechtliche Konsequenzen tragen und Entschädigungen für die betroffenen Anwender zahlen, allerdings hatte dieses Verfahren auch sehr starke Präsenz in den Medien. Es ist durchaus vorstellbar, dass zukünftige andere Verfahren bei ‚kleineren Vergehen' weniger Aufmerksamkeit erlangen.

Die TCPA-Panik des Jahres 2003 hat sich gelegt. Betrachtet man die Entwicklung, so lässt sich absehen welche der damaligen Befürchtungen mehr oder weniger realistisch sind. Es muss allerdings festgestellt werden, dass die damals beschriebenen Szenarien vom technischen Standpunkt heute oder in Bälde durchaus realisierbar wären. Die entsprechenden TPM Module haben sich auf neuere Plattformen verbreitet und welche Funktionalitäten damit durchgesetzt werden sollen, wird sich eventuell zum ersten Mal mit Windows Vista zeigen.

6.2 Ausblick – die Zukunft von DRM und Trusted Computing

Noch mögen die Benutzer von massiv beworbenen Online-Musikanbietern wie z. B. musicload.de zufrieden sein. Sollten sie aber demnächst einen neuen MP3-Player,

einen iPod oder gar einen zune erwerben und feststellen, dass die alten Daten unbrauchbar sind, wird sich die Meinung schnell ändern.

DRM hat sich gerade erst weiter verbreitet und die Einschränkungen für die Nutzer werden vielen erst langsam klar. So lange für viele Anwender die bloße Idee, Lieder einzeln im Internet zu kaufen, noch neu ist, fällt dies aber eher weniger ins Gewicht.

So lange es keine gemeinsamen Standards für DRM gibt, also iPod, zune und andere die gleichen Daten abspielen können, werden die unerwünschten Eigenschaften von DRM allerdings auf Dauer offensichtlicher. Wenn die ‚Gängelei' der Nutzer überhand nimmt, wird sich zwangsläufig eine stärkere alternative Richtung abzeichnen.

Vielleicht findet aber auch ein Umdenken statt und der Kampf der Industrie gegen die Tatsache, dass sich geistiges Eigentum heute schneller um den Erdball verbreiten lässt, entschärft sich? Sollte es zu der von vielen geforderten ‚Flatrate' kommen? Die Versuche der Industrie, an dem seit dem 19. Jahrhundert existierenden Vertriebsweg des Datenträgers, der urheberrechtlich geschützten Inhalt enthält und somit verkauft werden kann, festzuhalten, werden wohl einer Erneuerung unterzogen werden müssen. Auch hier wird sich ein Wandel abzeichnen, denn das System wird auf Dauer nicht standhalten.

Oder in mittlerer Zukunft setzt sich vermehrt das Streaming durch? Mithilfe von verbesserten Übertragungstechnologien von GPRS über UMTS, wachsenden WLan-Hotspots bis WiMax wird es zukünftig vielleicht interessanter, seinen Musiksammlung online aufzubewahren und jederzeit darauf zugreifen zu können?

In einem Kommentar zu dem 2002 erschienenen Artikel zum Thema „TCPA and Palladium: Sony Inside"[31] schreibt „Xeriar"

[31] http://www.kuro5hin.org/story/2002/7/9/17842/90350

> I get the feeling that this will end up being very one-sided in the end. Either corporations lock nearly everything down, via laws, treaties and technology, or the free market chooses the other route and makes them all irrelevant.
>
> I would like to think that ~4 years is a sufficient timetable for the latter outcome to be quite likely. It may be that I am also an optimist - we shall see.

Vielleicht müssen wir doch noch mal '~4 years' warten, bis wir absehen können, wohin die Reise geht.

Quellenverzeichnis

Letting Loose the Light: Igniting Commerce in Electronic Publication. In: Stefik, M., ed. Internet Dreams: Archetypes, Myths, and Metaphors, MIT Press, Cambridge, MA, 1996