

Cross Media
Digital Rights Management
Ausarbeitung zum Vortrag

André Kloth <kloth@cs.uni-potsdam.de>
Michael Augustin <augustin@math.uni-potsdam.de>
Stefan Kröger <kroegers@cs.uni-potsdam.de>
Stephan Uhlmann <su@su2.info>

6.2.2004

Institut für Informatik
Universität Potsdam



Copyright © 2004

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts and no Back-Cover Texts. A copy of the license can be obtained from <http://www.gnu.org/copyleft/fdl.html>.

Inhaltsverzeichnis

1	Status und Ziele	4
1.1	Definition	4
1.2	Status	4
2	DRM auf Cross Media	6
3	Rechtliche vs. technische Umsetzung	9
3.1	Einleitung	9
3.2	Historie	9
3.3	Problematik der Umsetzung	10
3.4	Rechteverwaltung	11
3.4.1	Nutzungsrechte	11
3.4.2	Transportrechte	11
3.4.3	Bearbeitungsrechte	11
3.5	Fazit	12
4	Trusted Computing	13
4.1	Einleitung	13
4.2	Technischer Hintergrund	14
4.2.1	TPM Funktionseinheiten	14
4.2.2	TPM nicht-flüchtiger Speicher	14
4.2.3	TPM flüchtiger Speicher	15
4.3	Lösungen	15
4.4	Showcase	15

4.5	Diskussion	16
4.6	Ausblick	17
5	Quellen	18
6	Bilderverzeichnis	20

Kapitel 1

Status und Ziele

1.1 Definition

Bei Digital Rights Management Systems (DRMS) handelt es sich um elektronische Vertriebssysteme für digitale Inhalte. Bilder, Musik, Videos, Texte und Programme sollen in dieser digitalen Infrastruktur an aktive und intelligente Copyrightinformationen gekoppelt sein. Damit ermöglicht man eine sichere Verbreitung und (insbesondere) Verwertung digitaler Inhalte on- und offline, z.B. über das Internet, mobile Abspielgeräte oder Telefone.

DRMS gestatten es dem Inhaber eines digitalen Werkes, eine effiziente und detaillierte Rechteverwaltung vorzunehmen und eröffnen damit die Möglichkeit neue Geschäftsmodelle für digitale Inhalte zu schaffen (z.B. Pay-Per-Use/-Listen/-View, Abonnementangebote, kostenpflichtige Downloads). Die Rechteinhaber digitaler Inhalte haben somit volle Kontrolle über diese. Das DRMS kann z.B. erfassen wer, wann, wie oft, zu welchem Preis und in welcher Art und Weise auf ein Werk zugegriffen und es somit genutzt hat. Diese stärkste Form von Digital Rights Management erlaubt eine individuelle Abrechnung der Nutzung.

Eine der grundlegendsten Technologien für DRM ist die Kryptographie, denn ohne eine technische Untermauerung der Rechte eines Autors an seinem digitalen Werk, bleibt das Werk nur eine Folge von Bits, die sich ohne Weiteres vervielfältigen und verändern lässt.

1.2 Status

Festzuhalten ist zunächst, dass es sich bei unseren heutigen Computern um Allzweckrechner mit Allzweckbetriebssystemen und Allzweckprogrammen handelt. Dank dieser Technik genießen wir jederzeit die Freiheit, Bits und Bytes beliebig zu manipulieren und zu kopieren (Gesetze allein sind nicht in der Lage, z.B. Raubkopieren oder Reverse En-

gineering zu unterbinden). Zusätzlich bietet das Internet eine ideale Plattform, digitale Inhalte ohne Qualitätsverlust auszutauschen.

Mittels technischer Verfahren wie digitale Wasserzeichen (Fingerprints), Verschlüsselung oder kryptographische Signaturen werden bereits auf verschiedene Art und Weise digitale Inhalte mit Nutzungsrechten versehen. Jedes System, das Verfahren eines DRMSs umsetzt, beinhaltet mindestens eine Blackbox-Komponente, die dem Nutzer verborgen bleibt und eben das o.g. Allzweckssystem um eine ungewünschte Komponente kastriert (erst dann spricht man von einem Trusted System, das sich in einem kontrollierten Zustand befindet).

Im einfachsten Fall heute verwendeter DRM-Mechanismen erkennt zum Beispiel das in Adobe Photoshop eingebaute Counterfeit Deterrence System, ob ein Nutzer versucht, Geldscheine mit dem Bildbearbeitungsprogramm zu editieren (der Begriff Geldscheine kann hier auch z.B. durch lizenzt rechtlich geschütztes Bildmaterial ausgetauscht werden) und verhindert es.

Das von Adobe 1993 eingeführte Portable Document Format (PDF) um gestaltete Textdokumente über das Internet zugänglich zu machen, erlaubt bereits innerhalb der PDF-Kodierung, den Zugang zum Text mit einem Passwort zu schützen und einzelne Operationen wie Drucken, Verändern, Auswahl und Kopieren einzelner Passagen zu unterbinden. So können beispielsweise bei Amazon E-Books heruntergeladen, die maßgeschneidert für Kunden mit registriertem Acrobat Reader (Software zum Betrachten von PDFs) sind. Der Verlag legt dabei fest, in wie weit man z.B. das Recht hat, das Buch auszudrucken, vorlesen zu lassen, auf einen anderen Rechner zu überspielen, etc. Dabei verweist Amazon darauf, dass aufgrund der Beschaffenheit der Ware [...] E-Books von der Rückgabe und vom Umtausch ausgeschlossen sind.

Das von Matsushita und Toshiba entwickelte Content Scrambling System (CSS) dient dazu, voraufgezeichnete DVD-Videoinhalte vor unbefugtem Abspielen zu schützen. Ausser, dass das Abspielen an einem nicht autorisierten Player scheitern kann, kommt hinzu, dass man sich eventuell in einem falschen Teil der Welt aufhält (Regional Playback Control).

Microsoft hat mit dem Microsoft Windows Media® Rights Manager einen Weg für alle Anbieter von multimedialen Inhalten geschaffen, z.B. Filme die vom Windows Media Player® abgespielt werden können, mit bestimmten Nutzungsrechten zu versehen und im Internet zu bestimmten Nutzungsbedingungen anzubieten. Damit kann jeder Anbieter eigene Bezahlssysteme für seine multimedialen Inhalte erstellen und verwalten (Pay-per-Download und Pay-per-View sind nur zwei grobe Beispiele wie die Nutzungsbedingungen aussehen können).

Kapitel 2

DRM auf Cross Media

Der folgende Abschnitt beschreibt zu Beginn kurz einige grundlegende Neuerungen die das Digital Rights Management hervorgebracht hat. Des Weiteren werden Vor- und Nachteile dieser Entwicklungen diskutiert, woraufhin eine genauere Betrachtung des DRM-Ablaufmodells folgt. In diesem Zusammenhang wird abschließend das allgemeine DRM-Referenzmodell auf die Thematik Cross Media abgebildet und einige Beispiele angeführt.

Die Möglichkeit auf beinahe jedem digitalen Medium Information in unverfälschter Art und Weise zu vervielfältigen, stellt ein Problem für viele Content- Provider dar. Um Inhalte vor unerwünschter Duplizierung zu schützen, werden bereits heute unterschiedlichste Kopierschutzmechanismen wie Verschlüsselung und digitale Wasserzeichen in Bilder und Dokumente eingearbeitet. Ferner werden neue Ideen gesucht, mit denen die Nutzer von digitalen Inhalten ein kommerzielles Angebot sinnvoll verwenden können. So entstanden neue Geschäftsmodelle, welche dem Kunden in dem Maße entgegenkommen, dass dieser beispielsweise nicht mehr für überflüssige Angebote zahlen muss, sondern nur noch für das, was er eigentlich nutzen möchte. Zu nennen sind in diesem Zusammenhang Verfahren wie Pay- Per- View, kostenpflichtige Downloads und das Abonnieren von Inhalten. Vorteilhaft gestaltet sich bei diesen Modellen die Verwendung des Internets als preiswerter Distributionskanal, der Rund um die Uhr Angebote aus der ganzen Welt zur Verfügung stellt. Doch auch andere digitale Medien können in diesem Zusammenhang verwendet werden. Dabei ist lediglich zu unterscheiden, auf welchem Endgerät der Kunde die Information für seine Zwecke nutzen möchte. Um eine möglichst einheitliche Verwaltung der digitalen Rechte für die verschiedenen Übertragungsverfahren und eingesetzten Medien zu organisieren, werden Modelle erarbeitet, die im Großen und Ganzen ein DRM- Ablauf abstrahieren und vereinfachen.

Der eigentliche Sinn, der bei diesen Verfahren im Vordergrund steht, ist, mittels Zugangs- und Nutzungskontrollen den Nutzer zu veranlassen, für die bereitgestellten Inhalte zu zahlen. Der Schutz der Authentizität und Integrität von Angeboten ist dabei zwar nicht zu vernachlässigen, allerdings wohl eher nicht als Hauptanliegen zu nennen. So macht

sich die Industrie mittlerweile Gedanken darüber, wie sie dem Kunden nicht mehr nur softwarebasierte Decoder anbietet, sondern gegen Manipulation resistente Hardwarelösungen vertreibt. Nennenswerte Beispiele sind hier spezielle Authentifizierungsmethoden durch Computerchips (TPM) oder Smartcards, die bestimmte Informationen über einen Benutzer speichern sollen, um Lizenzen für digitale Angebote vergeben zu können. Um sich weiter vor der Missachtung von Urheber- und Lizenzrechten auf diesem Gebiet zu schützen, kommen Suchsysteme zum Einsatz, die das Auffinden unberechtigter Kopien ermöglichen sollen.

Betrachtet man das Referenzmodell für das Digital Rights Management von Internetinhalten, so wird man eine gewisse Ähnlichkeit bei vielen anderen Abläufen für die Rechteverwaltung finden. Denn die für das DRM essentiellen Bestandteile wie Content- Provider, License Server und Nutzer stehen für jedes digitale Medium im gleichen Zusammenhang. Bei dem DRM Referenzmodell für Internetinhalte ist es vorgesehen, dass sich der Nutzer von einem Content- Server bestimmte digitale Inhalte aus einem Content Repository herunterlädt. Dabei stehen ihm sämtliche Produktinformationen für seine Auswahl zur Verfügung. Durch die Aktivierung des DRM- Controllers beim Nutzer, sucht dieser die nötigen Informationen um eine Lizenz zu erstellen und sendet daraufhin an einen License-Server Identifikationsmerkmale des Anwenders und Inhaltes. Die Aufgabe des License-Servers besteht nun darin, zunächst den Nutzer zu identifizieren und dessen Rechteinformation zu bestimmen. Falls es für die benötigte Lizenz erforderlich ist, startet der License-Server eine finanzielle Transaktion und erstellt bei einer positiven Rückmeldung eine verschlüsselte Lizenz durch den Lizenz Manager, welche dann dem Nutzer zugeschickt wird. Die Verschlüsselung ist hierbei von Notwendigkeit, um zu gewährleisten, dass die Lizenz nicht von Dritten missbraucht werden kann. Hat der Nutzer die Lizenz erhalten, kann er nach der Entschlüsselung des digitalen Inhaltes und einer Freigabe an das Wiedergabegerät seine geforderte Information einsehen.

Dieser Ablauf ist wie bereits genannt für die einzelnen unterschiedlichen Medien sehr ähnlich, denn wer als Content- Provider agiert, oder auf welche Art sich der Benutzer die Lizenz organisiert ist auf vielerlei Weise möglich. Fest steht jedoch, dass durch die Vergabe der Lizenz der Umfang in dem sich der Benutzer bewegen darf festgelegt werden kann.

Lösungen der einzelnen Anbieter von Inhalten für unterschiedlichste Medien sind in diesem Zusammenhang die Abonnementsysteme im Internet, bei denen die gewünschte Information vom Nutzer für einen bestimmten Zeitraum angefordert werden kann. Dabei ist es wichtig, dass sich möglichst keine illegalen Kopien im Netz befinden, oder sich zumindest die Qualität der Information des Anbieters stark von der Kopie unterscheidet. Aber auch die Überlegung heruntergeladene Musikstücke nicht auf einem Massenspeicher beim Nutzer zu platzieren, sondern den heruntergeladenen Inhalt direkt an die Soundkarte weiterzuleiten, sind Ziele, die von den Entwicklern verfolgt werden. Andere Beispiele sind Geräte wie der Code Meter von Wibu- Systems, welcher eine integrierte Lösung für viele Hersteller darstellen soll. Dieser Code Meter ist eine Art USB- Stick, auf dem der Anwender verschiedene Nutzungsrechte und persönliche Informationen speichern kann. Der Vorteil liegt darin, dass die Nutzungsrechte flexibel beim Käufer bleiben und auf verschie-

denen Geräten abgerufen werden können. Napster bietet eine Softwarelösung, die als eine Art digitaler Umschlag für getauschte Dateien angesehen werden kann. Dadurch lässt sich beispielsweise nachvollziehen, welche Musiktitel getauscht werden oder reglementieren, welche Vorgänge (brennen von MP3- Dateien) vollzogen werden dürfen. Weiter lassen sich bereits bestehende DRM- Verfahren für den PC wie die Acrobat- Suite von Adobe auf kleinere Geräte wie Palms abbilden. Aber auch die Smart Card ist eine technische Möglichkeit für das DRM, die nach einem ähnlichen Modell wie der Code Meter arbeitet.

Kapitel 3

Rechtliche vs. technische Umsetzung

3.1 Einleitung

In diesem Abschnitt geht es um die rechtlichen Probleme im Zusammenhang mit DRM und den damit verbundenen Mechanismen. Die Idee eine Kontroll- und Verwaltungsform für digitale Informationen und Informationsträger zu schaffen ist bereits ein seit Jahren bestehendes Ziel der Industrie. Den Beteiligten geht es darum, „ihr“ Recht mit Hilfe von Schutzmechanismen wie DRM durchzusetzen. Mit dieser Problematik wird sich der folgende Teil der Ausarbeitung beschäftigen.

3.2 Historie

In den neuziger Jahren wandelte sich die Möglichkeit der Datenvervielfältigung enorm. So war es bis dato, nur schwer möglich Information mit geringen Kosten in großem Maße zu vervielfältigen. Informationen und geistige Eigentum, wie Bücher, Musik waren bis zum Durchbruch der Personal Computer und der CD auf dem Massenmarkt, für den Normalverbraucher, fast ausschließlich in analoger Form verfügbar. Also stellte auch die massenhafte Vervielfältigung von Datenträgern ein Problem dar. Das bedeutete, dass die Mechanismen zur Wahrung von Lizenzrechten und Urheberrechten leicht umzusetzen waren, etwas das Kontrollieren von Druckereien oder Tonträger- und Videoträgerproduktionsstätten. Eine Vervielfältigung durch den Normalverbraucher war nur mit Qualitätsverlust umsetzbar und wurde auch deshalb von den Rechteinhabern und dem Gesetzgeber für den Privatbereich erlaubt. Immer mehr Informationen standen jedoch mit den Jahren, auch in digitaler Form zur Verfügung und durch die Möglichkeit der digitalen Kopie, ohne Qualitätsverluste, wie etwa mit Hilfe der CD-R/RW oder ähnlichen Datenträgern. Gab es nun für den Verbraucher die Möglichkeit, sich kostengünstige Kopien von Informationen selber zu schaffen, anstatt sich diese zu kaufen oder Lizenzen für die Nutzung zu erwerben.

ben. Auch die Einführung diverser Kopierschutzmaßnahmen, etwa bei Musik CDs oder Video DVDs brachte keine Abhilfe, da findige Nutzer es immer wieder verstanden, diese Kopierschutzmechanismen auszuhebeln. Dies führte zu einem erheblichen Gewinnrückgang bei der betroffenen Industrie. Denn gerade die Musikindustrie hatte seit den achtziger Jahren extreme Gewinnzuwächse durch die Einführung der CD erhalten. Schnell hatte man sich darüber geeinigt, dass neue und strengere Gesetze zum Verbot, illegaler Kopien von Informationen notwendig waren.

Der erste Schritt wurde 1998 mit dem „Digital Millennium Copyright Act“ (DMCA) in den USA gemacht. Mit dem Verbot des Umgehens von Kopierschutzmaßnahmen, gab es von nun an in den USA eine rechtliche Grundlage für die Strafverfolgung von Personen. Jedoch blieb die Frage nach der Durchsetzung des Gesetzes offen. Wer und wie sollte man die Einhaltung des Gesetzes kontrollieren? Ein weiterer kritischer Fakt war und ist die Globalität des Problems. So hatte der DMCA zwar Auswirkungen auf US Bürger, schränkte jedoch EU-Bürger, beispielsweise nicht ein. Daraufhin gab es auch ab 1999 von der EU Initiativen zur Reformierung des Urheberrechts in den einzelnen Mitgliedstaaten. Dafür wurde ab Mai 2001 die Richtlinie 2001/29EG „zur Harmonisierung bestimmter Aspekte des Urheberrechtes und der verwandten Schutzrechte in der Informationsgesellschaft“ herausgebracht und somit von den Mitgliedstaaten eine Anpassung des geltenden Rechts gefordert. Im April 2003 wurde in Deutschland ein Gesetzesentwurf zum Urheberrecht verabschiedet. Jedoch sind bis heute noch Unstimmigkeiten und Unklarheiten enthalten. Eine wirkliche Harmonisierung und gleiche Gesetze in Europa oder gar weltweit, liegen dabei jedoch noch in sehr ferner Zukunft.

3.3 Problematik der Umsetzung

Die Schwierigkeit ein derartiges Gesetz zu verabschieden, liegt in den kontroversen Vorstellungen der Betroffenen. So gibt es auf der einen Seite die Vertreter der Industrie und auf der anderen die Verbraucherschutzbeauftragten und andere Interessengruppen. Bleibt also die Frage zu klären, was geschützt werden soll und wie. Nach Ansicht der Verbraucherschutzbeauftragten muss es dem einzelnen auch in Zukunft gestattet sein, Sicherheitskopien von erworbenen Informationen in beliebiger Form anlegen zu können. Jedoch ist dies oftmals nicht möglich, ohne Kopierschutzmechanismen zu umgehen und gegen geltendes Recht zu verstoßen. Es ist nur erlaubt Kopierschutzmechanismen zu umgehen, um eine erworbene Produkt funktionsfähig zu machen, nicht aber um sich beispielweise ein Sicherheitskopie anzufertigen. Auch stellen die momentan von der Industrie verwendeten Mechanismen weitere Probleme in den Raum, so ist z.B. die Nutzung gekaufter CD nur unter bestimmten Umständen möglich. Wenn etwa das CD-Abspielgerät ebenso mit Untätigkeit auf den Kopierschutz reagiert, wie das Kopiergerät, so ist eine Nutzung nicht möglich. Die Vertreter der Industrie argumentieren dagegen mit hohen Verlusten, durch die illegale Weitergabe von Kopien an Dritte. Gerade die nicht vorhandenen Kontrollmechanismen zur Nutzung von Kopien und Sicherheitskopien stellt für sie ein Hauptproblem

dar. Diese Kontrollmechanismen bergen natürlich Risiken und Gefahren und bedürfen einer rechtlichen Grundlage. Wer darf Überwachen und kontrollieren, wie darf man Überwachen und wer kümmert sich um den Ordnungsgemäßen Umgang mit den gewonnenen Informationen. Denn für die Industrie würden solchen Informationen natürlich auch für andere Interessen von hoher Bedeutung sein. Verfügt man z.B. über die Hörgewohnheiten von Anwendern oder sogar über Daten wie: „Wann nutzt Wer Was?“, so ließen sich diese Informationen hervorragend für gezielte Werbung oder Verbraucheranalysen und darauf basierende Marktstrategien anwenden.

3.4 Rechteverwaltung

Bei DRM geht es nicht nur darum digitale Informationen vor der illegalen Vervielfältigung zu schützen, sondern auch um die Frage, was ich mit ihnen machen darf und was nicht. Dafür lassen sich die Rechte in 3 Gruppen unterteilen.

3.4.1 Nutzungsrechte

In welcher Form darf der Konsument die erworbenen Informationen nutzen. Diese Problematik findet sich z.B. bei eBooks wieder, darf der Käufer diese auch ausdrucken oder nur am Bildschirm lesen, darf er die Information immer und zeitunabhängig nutzen oder unterliegt die Nutzung eventuellen Regelungen, die nur eine bestimmte Nutzungsarten und Nutzungszeiträume erlauben.

3.4.2 Transportrechte

Gerade die Portabilität von digitalen Informationen wird heute immer wichtiger. Doch beim Portieren ist es schwer festzustellen in welcher Form und wohin etwas transportiert wird. So muss also geregelt werden, ob man Informationen geräteabhängig erwerben muss oder, ob es möglich ist die Informationen auf verschiedenen Geräten des gleichen Endnutzers zur Verfügung zu stellen. Regelungen zum Kopieren, Verschieben und Verleihen von Informationen sind hier vonnöten und sollen durch DRM-Mechanismen möglich werden. So könnte z.B. die Lizenzierung von Software hardwareabhängig gestaltet werden.

3.4.3 Bearbeitungsrechte

Hier stellt sich ein altes Problem dar. Das Bearbeiten von urheberrechtlich geschützten Informationen ist schon seit langen ein Problem und könnte mit geeigneten Maßnahmen sogar in eine neue eindeutigere Form gebracht werden. Es stellt sich immer die Frage in

wie weit Informationen wiederverwendet werden dürfen und welche Kennzeichnungen im Falle einer Wiederverwendung vonnöten sind. So wird es mit DRM-Mechanismen möglich sein, gezielt die Verwendung von Informationen einzuschränken. Man beginnt mit der Steuerung des Gebrauchs, durch Festlegung, ob es erlaubt ist Teile des Dokumentes zu nutzen (Cut&Past) oder ob man vielleicht Ergänzungen oder Veränderungen vornehmen darf, kann durch Mechanismen geregelt werden, auch das Problem des Zitierens ohne Quellenangabe kann durch geeignete Mechanismen gelöst werden, da man sogar in der Lage sein könnte die Geschichte und Herkunft eines Dokumentes zu jedem Zeitpunkt festzustellen.

3.5 Fazit

Die Anpassungen des Urheberrechts und den damit verbundenen Schutzmaßnahmen von Rechteinhabern wird noch eine Zeit brauchen und selbst wenn dieser Schritt entgeltig getan ist, geht es daran nationales Recht und internationale Richtlinien zu vereinen. Solange dies nicht geschehen ist, wird auch die rechtliche Grundlage für DRM-Mechanismen nicht auf sicherem Fundament stehen. Die Durchsetzung und die Akzeptanz der Nutzer hängt von einer gesicherten Rechtslage ab. Denn die Möglichkeiten der Kontrolle und Limitierung der Nutzung die mit DRM ermöglicht, beherbergen auch Risiken. So wäre es auch vorstellbar Informationen nur ausgewählten Gruppen zur Verfügung zu stellen oder von Seiten der Betreiber, Rechteinhaber/Rechteverwalter sogar Informationen im Nachhinein zu entfernen oder verfälschen. Alldies bedarf einer verstärkten Reglementierung und Absicherung, sowie einer fortwährenden Beobachtung durch Unabhängige.

Kapitel 4

Trusted Computing

4.1 Einleitung

Trusted Computing bezeichnet die Bestrebungen einen Standard für einen sicheren PC zu schaffen. Die „Sicherheit“ bezieht sich hier jedoch eher auf die „Vertrauenswürdigkeit“ eines PC, die man hauptsächlich gegenüber Dritten belegbar machen möchte. Daher auch „Trusted Computing“.

Um dieses Ziel zu erreichen, bildete sich die Trusted Computing Group (TCG). Dies ist ein Konsortium verschiedener Hersteller von Computern und Computer-Chips sowie Softwareunternehmen wie Microsoft, Intel, IBM, HP, u.v.a.. Die Gruppe geht aus der ehemaligen Trusted Computing Platform Alliance (TCPA) hervor, die dieser Bewegung den Namen gab. Unter dem Kürzel TCPA findet man weiterhin viele Quellen im Internet.

Die TCG veröffentlicht nun diese Standards, die ein so genanntes kryptographisches Subsystem definieren. Kernelement und der Chip zur Umsetzung des Standards auf Hardwareseite ist das Trusted Platform Module (TPM). Dies ist ein fest auf dem Mainboard eines Computers verdrahteter bzw. später sogar in die CPU integrierter Chip. Er ist vergleichbar mit einer Smart Card, soll jedoch im Unterschied zu dieser nicht eine Person oder einen Benutzer identifizieren, sondern eine „Plattform“ also einen bestimmten Computer mit einem bestimmten Betriebssystem. Das TPM ist auch bekannt unter dem Namen „Fritz-Chip“, benannt nach dem US-Senator Fritz Hollings, der mit dem Consumer Broadband and Digital Television Promotion Act (CBDTPA) einen Gesetzentwurf in den US-Senat eingebracht hat, der verpflichtende Kopierschutzsysteme für alle kopierfähigen digitalen Geräte vorsieht.

4.2 Technischer Hintergrund

Das TPM in seiner Architektur aus drei Komponenten:

1. die Funktionseinheiten
2. der nicht-flüchtige Speicher
3. der flüchtige Speicher

4.2.1 TPM Funktionseinheiten

Das TPM enthält einige Funktionseinheiten für seine für seine kryptographischen Fähigkeiten benötigt werden. Dazu zählen ein Zufallszahlengenerator, eine Hash-Einheit (SHA-1 Algorithmus), eine HMAC-Einheit, eine Einheit zur RSA-Schlüsselerzeugung (bis 2048 Bit Schlüssellänge) sowie eine Einheit zur RSA-Ver- und Entschlüsselung und Signierung von Daten.

Diese Funktionen können also on-chip erledigt werden. Sie können damit vom Rest des Systems abgeschottet und bei Bedarf hardwarebeschleunigt ausgeführt werden.

4.2.2 TPM nicht-flüchtiger Speicher

Der nicht-flüchtige Speicher enthält Daten, die auch nach einem Reset erhalten bleiben (in der Praxis durch ein EEPROM realisiert). Von zentraler Bedeutung ist dabei der Endorsement Key (EK), ein 2048 Bit RSA-Schlüssel, der bei der Herstellung des Chips zufällig erzeugt wird und an das TPM gebunden wird. Er identifiziert damit den Computer mit diesem TPM eindeutig. Der Endorsement Key kann normaler Weise nicht entfernt werden. Die neue Version 1.2 der TPM Spezifikation sieht jedoch auch die Möglichkeit der Löschung des EK vor.

Der zweite wichtige Schlüssel im nicht-flüchtigen Speicher ist der Storage Root Key (SRK), ebenfalls ein 2048 Bit RSA-Schlüssel. Er wird bei der initialen Besitzübernahme des Systems (und damit des TPMs) durch den Benutzer erzeugt. Der private Schlüssel des SRK verlässt das TPM nicht. Der öffentliche Schlüssel kann exportiert werden, z.B. damit Dritte damit Daten verschlüsseln oder Signaturen überprüfen können. Mit dem SRK werden eigene Schlüssel verschlüsselt, wenn sie in das TPM importiert werden („wrapping“).

Ebenfalls im nicht-flüchtigen Speicher befindet sich das Owner Auth Secret, das zusammen mit dem SRK erzeugt wird und der Autorisierung von sensitiven Kommandos dienen soll.

4.2.3 TPM flüchtiger Speicher

Der flüchtige Speicher eines TPM hat zehn „Slots“ zur Speicherung von selber erstellten RSA-Schlüsseln (bis 2048 Bit). Diese Funktion eines sicheren Schlüsselspeichers ist eine der zentralen Aufgaben des Chips.

Des weiteren enthält der flüchtige Speicher 16 sog. Platform Configuration Register (PCR). Diese Register enthalten 160 Bit Hashes, die der Überprüfung der Software-Integrität dienen. Es werden beim Starten des Systems sukzessiv über alle zu startenden Komponenten (BIOS, MBR-Code, Kernel, ...) Hashes gebildet und geprüft, ob der Hash-Wert noch dem erwarteten Wert entspricht. D.h. eine Komponente kann überprüfen, ob eine Komponente ausgetauscht oder anderweitig verändert wurde.

Die weniger wichtigen Key Handles und Auth Session Handles im flüchtigen Speicher dienen der temporären Speicherung von Namen für Schlüssel und Authorisations-Zuständen über mehrere Kommandos hinweg.

4.3 Lösungen

Die TPM Spezifikation wurde schon in zwei Chips umgesetzt, dem AT97SC3201 von Atmel und dem SLD 9630TT1.1 von Infineon. Ersterer wurde schon in der Microsoft Xbox und in allen IBM Thinkpad Notebooks seit Oktober 2002 eingebaut. Microsoft wird in der kommenden Windowsgeneration „Longhorn“ seine „Next Generation Secure Computing Base for Windows“ (NGSCB, auch „Palladium“ genannt) mit einfließen lassen, die die TCG-Spezifikation im Betriebssystem umsetzt. American Megatrends stellt mit dem AMIBIOS8 ein TCG-konformes BIOS her. Für Linux gibt es schon Kernelmodule welche den TPM benutzen, z.B. um ein sicheres Dateisystem zu implementieren. IBM stellt ein Linux-Toolkit zur Verfügung, mit dem man die wichtigsten Funktionen des TPM in seinen Thinkpads nutzen kann (siehe Showcase).

4.4 Showcase

Die Bilder 1 und 2 im Bilderverzeichnis zeigen Protokolle einer Demonstration der verschiedenen Testprogramme aus dem IBM Linux-Toolkit zum Testen der TPM-Funktionen. In Bild 1 wird eine Datei verschlüsselt, wieder entschlüsselt (sealfile/unsealfile), ein eigener RSA-Schlüssel erzeugt (createkey), dieser ins TPM importiert (loadkey) und damit eine Signatur einer Datei gebildet, die danach überprüft wird (signfile, verifyfile). Bild 2 zeigt die Ausgabe von tcpa_demo, welches den Inhalt der PCR-Register anzeigt und die Anzahl der belegten Schlüssel in den „key slots“ sowie deren Handles. Der Befehl evict-key löscht diese Schlüssel.

4.5 Diskussion

Trusted Computing ist ein sehr aktuelles Thema, bei dessen Diskussion es verschiedene Argumente der Befürworter und der Gegner gibt. Dafür spricht, dass das TPM als sichere Schlüsselaufbewahrung sicherlich positiv zu bewerten ist. Auch die Möglichkeit Dokumente (z.B. geheime) an ein System zu binden, ist für bestimmte Anwendungsgebiete sicherlich von Vorteil. Hersteller freuen sich über die Möglichkeit zur Überprüfung der (in ihren Augen) Vertrauenswürdigkeit eines PC (remote attestation). Trusted Computing ist also erstmal an sich nichts Schlechtes, sondern kann eben für gute und für schlechte Anwendungen genutzt werden. IBM betont sehr deutlich, dass TC nicht mit NGSCB oder mit DRM gleichzusetzen sind, dies sind Anwendungen von TC, welche man kritisieren kann, ohne jedoch TC insgesamt kritisieren zu müssen.

Die Gegner wollen jedoch genau diese Anwendungen von TC nicht so strikt getrennt diskutieren, denn sie sind der Meinung, man sollte zu einer neuen Technologie auch deren geplante Anwendungen betrachten. DRM stellt sicher eine dar. Es wird aber auch die Entmündigung des Benutzers beklagt, denn dieser hat über Teile seines PC nicht mehr die vollständige Kontrolle (nämlich den Teil mit dem Endorsement Key im TPM). Das Merkmal des remote attestation bereitet auch Unbehagen, da Dritte damit den Zustand des eigenen Systems abfragen können, was nicht immer gewollt ist.

Problematisch ist auch, dass der Hersteller des TPM Zugriff auf den Endorsement Key hat, denn damit hat er im wahrsten Sinne des Wortes den Schlüssel zum TPM in der Hand. Dies ist ein wichtiger Punkt, den man beachten sollte, bevor man alle seine persönlichen Daten mit Schlüsseln aus dem TPM verschlüsselt.

Die Frage, wie man sich gegen Backdoors absichern kann, über die der Endorsement Key evtl. doch nach aussen gelangen kann, ist da ebenso wichtig. Auch wenn Microsoft beteuert niemals freiwillig („never voluntarily“) geheime Zugänge zum TPM zu installieren, werden sie sich jedoch dem Druck der Strafverfolgungsbehörden und Geheimdienste ausgesetzt sehen, die ein Interesse daran haben, dass Kommunikation unverschlüsselt abläuft. Im Zweifelsfall müssen sie dann eben unfreiwillig die Backdoor doch einbauen.

Probleme kann es auch für freie Software geben, für die es schwierig bis unmöglich ist, offizielle Zertifikate zur Signierung ihres Programmcodes zu erhalten.

Ganz grundsätzlich sind die Gegner der Initiative nicht darüber erfreut, dass Hersteller zwar ein Vertrauen zum System, mit dem man arbeitet, aufbauen wollen, dem Benutzer dabei jedoch stets misstrauen und der Benutzer in diesen Szenarien immer als „Feind“ angesehen wird.

Der Chaos Computer Club (CCC) in Deutschland und die Electronic Frontier Foundation (EFF) stellen bestimmte Forderungen, um Trusted Computing benutzerverträglich zu gestalten. Dazu zählt die Forderung nach einer vollständigen Kontrolle über alle Schlüssel im TPM (speziell dem EK), keine verborgenen Kanäle über die der EK nach außen gelangen könnte, eine Möglichkeit der Übertragung der Schlüssel im TPM auf andere PCs,

sowie die Transparenz der Zertifizierungs-Mechanismen. Die EFF fordert den Möglichkeit des sogenannten „owner override“. Nicht zuletzt aufgrund diesen öffentlichen Druck hin, wurde die TCG-Spezifikation kürzlich geändert und sieht jetzt auch die Möglichkeit der Löschung des Endorsement Keys vor. Das ist schon ein Schritt in die richtige Richtung, nur ist unklar, ob das in der Praxis auch von Privatanwendern durchgeführt werden kann, denn einen neuen (offiziell zertifizierten) EK zu erstellen und ins TPM aufzunehmen, dürfte mit einigem Aufwand verbunden sein. Das neue Direct Anonymous Attestation erlaubt das Erstellen verschiedener Attestation Identity Keys (AIK), mit denen man auf verschiedene Anfragen mit verschiedenen (pseudonymen) Identitäten antworten kann. Dies ist eine durchaus positive Sache.

4.6 Ausblick

Wie könnte nun die Zukunft aussehen? Gut ist sicherlich, eine sichere Schlüsselaufbewahrung zu haben. Gut wäre auch, wenn die Versprechungen einiger Hersteller sich bewahrheiten würden, dass es keine unsichere Software (Viren, Trojaner, bufferoverflows, ...) mehr geben wird. Dies ist sicher mit Vorsicht zu genießen, denn die Möglichkeit Software in vertrauenswürdige und nicht-vertrauenswürdige Software einzuteilen, macht sie ja nicht automatisch sicherer. Man könnte die Hoffnung haben, dass nach der Durchsetzung von DRM-Systemen, Produzenten vielleicht nicht mehr das Bedürfnis haben, vermeintliche finanzielle Verluste, die durch unberechtigtes Kopieren entstanden sind, ausgleichen zu müssen, was Inhalte billiger werden lassen könnte. Nicht zuletzt wäre eine Diskussion darüber positiv, was für *Rechte* denn DRM eigentlich „managen“ soll. Denn eigentlich scheint es ja doch um die Beschneidung von Rechten zu gehen.

Dies würde eindeutig zu schlechten Zukunftsszenarien gehören. Ebenso die Überwachung durch Hersteller und Inhaltenanbieter, die noch mehr Daten über einen Benutzer sammeln können. Trusted Computing ist dazu geeignet Wünsche von Dritten gegen den Willen des eigentlichen PC-Besitzers durchzusetzen. So kann das z.B. zum sog. „application lock-in“ führen, was bedeutet, dass ein Benutzer gezwungen ist ein bestimmtes Programm einzusetzen, um seine Dateien lesen zu können. Über die Gewährung oder Nicht-Gewährung von signierten Zertifikaten ist es möglich, dem Benutzer Migrations- und Backuprestriktionen aufzuerlegen, oder Up- und Downgrades zu erwingen. Ein einmal erzwungenes Vertrauensverhältnis zwischen Hersteller und Benutzer kann auch dazu mißbraucht werden, Spyware auf dem Computer zu installieren. Die Möglichkeiten von Trusted Computing und DRM sind endlos.

Eine etwas humoristische Vision von DRM zeigt Bild 3.

Kapitel 5

Quellen

- Volker Grassmuck, „Freie Software - Zwischen Privat- und Gemeineigentum“, Bundeszentrale für politische Bildung, Bonn, 2002
- Dr. T. Jaeger, Dr. A. Metzger, Publikationen vom Institut für Rechtsfragen der Freien und Open Source Software, <http://www.ifross.de>, Stand: Oktober 2003
- MPEG-4, Low Delay Advanced Audio Coding (AAC-LD), http://www.iis.fraunhofer.de/pub_rel/presse/2001/ifa/audio_d.html
- Robert A. Gehring, „DRM-Systeme im Spannungsfeld von Technik, Ökonomie, Recht und Politik“, September 2003, Paderborn, IHK Ostwestfalen-Lippe, <http://ig.cs.tu-berlin.de/ap/rg/2003-09/Gehring-DRM-Folgen-92003.pdf>
- Martin Brüggemann & Hendrik Zellmer, „Digital Rights Management“, Vortrag an der Universität Potsdam, 29.01.2004
- <http://www.privatkopie.net>
- Gerald Himmelein; „Ganz im Vertrauen“, c't Magazin 9/2003
- Prof. Dr. Francesco P. Volpe, David Bär; „Die Un-CDs“, c't Magazin 7/200
- Gerald Himmelein; „Blick ins Schloss“, c't Magazin 12/2003
- Richard Sietmann; „Durchmarsch mit DRM“, c't Magazin 22/2003
- Michael Plura; „Schlossgespenst“, c't Magazin 26/2002
- Georg Schnurer; „Nach- und nachgebessert“, c't Magazin 05/2003
- Michael Plura; „Eine Prise Sicherheit“, c't Magazin 05/2003
- Stefan Krempel; „Versiegelt in Krypto-Flaschen“, c't Magazin 05/2003

- Gerald Himmelein; „Ganz im Vertauen“, c't Magazin 06/2003
- Trusted Computing Group <https://www.trustedcomputinggroup.org/>
- „Trusted or Treacherous?“, Vortrag von Rüdiger Weis und Andreas Bogk auf dem Chaos Communication Congress 2003, <http://www.ccc.de/congress/2003/fahrplan/event/542.de.html>
- „Trusted Computing: Promise and Risk“, Seth Schoen, Electronic Frontier Foundation, http://www.eff.org/Infra/trusted_computing/20031001_tc.php
- „Take Control of TCPA“, Safford/Kravitz/Doorn, <http://www.linuxjournal.com/article.php?sid=6633>
- „TCPA Device Driver for Linux“, IBM Watson Research - Global Security Analysis Lab, <http://www.research.ibm.com/gsal/tcpa/>

Kapitel 6

Bilderverzeichnis

Bild 1, Protokoll der Demonstration des IBM Linux-Toolkits

Bild 2, Protokoll der Demonstration des IBM Linux-Toolkits

Bild 3, mögliches DRM-Zukunftsszenario, Bild von Perry Hoberman

```

susi:~/down/TPM/examples # ./sealfile
Usage: sealfile <key handle in hex> <key password> <data password> <input file>
<outputfile>
susi:~/down/TPM/examples # ./sealfile 40000000 srk mypass test.txt test.enc
susi:~/down/TPM/examples # ./unsealfile
Usage: unsealfile <key handle in hex> <key password> <data password> <input file
> <outputfile>
susi:~/down/TPM/examples # ./unsealfile 40000000 srk mypass test.enc test.unenc
susi:~/down/TPM/examples # md5sum test.txt test.enc test.unenc
2a53da1a6fbfc0bafdd96b0a2ea29515 test.txt
55a4ea651371584d741ae89dab76e238 test.enc
2a53da1a6fbfc0bafdd96b0a2ea29515 test.unenc
susi:~/down/TPM/examples # ./createkey
Usage: createkey <parent key handle in hex> <parent key password> <new key name>
<new key password>
susi:~/down/TPM/examples # ./createkey 40000000 srk mykey mypass
Created key with name mykey
susi:~/down/TPM/examples # ./loadkey
Usage: loadkey <parent key handle in hex> <parent key password> <key name>
susi:~/down/TPM/examples # ./loadkey 40000000 srk mykey
loaded key mykey, returned handle 138502
susi:~/down/TPM/examples # ./signfile
Usage: signfile <key handle in hex> <key password> <input file> <outputfile>
susi:~/down/TPM/examples # ./signfile 138502 mypass test.txt test.sig
susi:~/down/TPM/examples # ./verifyfile
Usage: verifyfile <sig file> <data file> <pubkey file>
susi:~/down/TPM/examples # ./verifyfile test.sig test.txt mykey.pem
Verification successful
susi:~/down/TPM/examples # □

```

Bild 1, Protokoll der Demonstration des IBM Linux-Toolkits

```

susi:~/down/TPM/examples # ./tcpa_demo
TPM successfully reset
TPM version 1.1.0.6
16 PCR registers are available
PCR-00: D1 74 26 E9 EC F9 02 29 96 1C B6 BE 47 18 C2 20 87 39 87 4D
PCR-01: C2 0D 98 6D 4A E0 53 67 F5 2F 06 0F 66 15 51 C1 38 0C AB 5A
PCR-02: EB B3 BA AE E7 57 4B B6 37 AA AB 67 0F 9A C1 BC EB 6F 80 F3
PCR-03: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-04: 30 89 C3 EC 42 6E 1D A7 20 C5 97 CA 9E EC 0D CF 73 E6 05 91
PCR-05: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-06: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-07: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-08: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10 Key slots are available
Key Handle 611E00 loaded
Key Handle 615001 loaded
Key Handle 138502 loaded
susi:~/down/TPM/examples # ./evictkey all
Key Handle 611E00 being evicted
Key Handle 615001 being evicted
Key Handle 138502 being evicted
susi:~/down/TPM/examples # □

```

Bild 2, Protokoll der Demonstration des IBM Linux-Toolkits

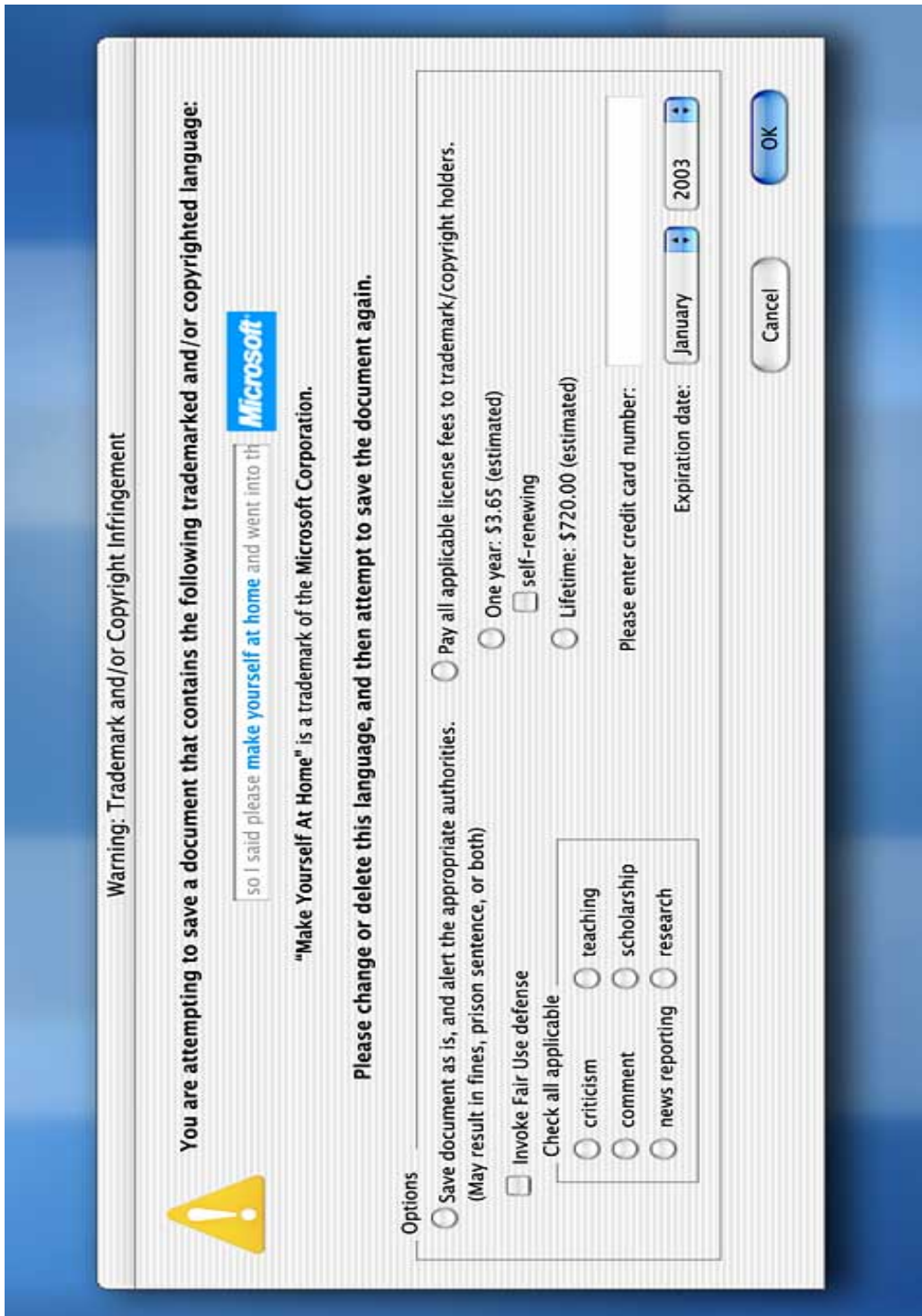


Bild 3, mögliches DRM-Zukunftsszenario, Bild von Perry Hoberman