Hauptseminar Musikalische Datenbanken

Thema 9: DRM-Verfahren

Prinzipen des Digitalen Rechtemanagements von Musik

Seminararbeit

Sebastian Wehrmann
Di 06.12.2005

Inhaltsverzeichnis

Kapitel 1

Einführung Digitales Rechtemanagement

Voranstellen möchte ich, dass es in dieser Ausarbeitung nur um audiobasierte DRM-Verfahren geht. DRM ist weit mehr, als nur der Schutz von Tonaufnahmen, doch darauf sei hier nur verwiesen.

1.1 Die Geschichte des DRM

Schon vor dem Einzug des Computers in die Haushalte blühte das illegale Kopieren von Musik. Damals wurde noch analog von Radio auf Kassette oder Kassette auf Kassette überspielt. Die Qualität war schlecht, aber man war es ja nicht anders gewöhnt. Und wollte man seine Musik doch in einer ansprechenden Qualität hören, fiel einem der Griff ins Portemonaie nicht schwer.

Doch heute, mit dem Einzug des Computers in fast jeden Haushalt, hat sich die Situition verändert. Ein PC mit integriertem CD-Brenner ist ohne technische Schutzmaßnahmen in der Lage, eine CD in Minuten 1-zu-1 zu kopieren. Und das ohne Qualitätsverluste. Es ist also nicht weiter verwunderlich, dass sich viele die CDs von Freunden geliehen haben, um sich selbst eine Kopie zu erstellen.

Verschärft wurde diese Situation durch die weite Verbreitung des Breitband-Internet und die fallenden Preise bei MP3-Playern. In s.g. Tauschbörsen wurde Musik zum Großteil im MP3-Format ohne jegliche Probleme getauscht. Jeder bot seine Musik an, und lud sich die Lieblingsmusik von fremden Leuten auf der ganzen Welt auf seinen Rechner. Und auch hier war dann der Weg zur eigenen CD nicht weit.

Seit Ende der 90er Jahre versuchen nun die großen Musikkonzerne den Anwender in der Nutzung seiner gekauften Musik zu beschränken. Es begann mit dem von vielen Anwendern gehassten Kopierschutz auf CDs, der vor allem zur Folge hatte, dass diese CDs in einem PC-Laufwerk nicht mehr abspielbar waren. Teilweise gab es sogar Probleme mit älteren CD-Playern, die diese neuen kopiergeschützten CDs nicht erkannten und sich weigerten, die teuer gekaufte Musik abzuspielen. Doch selten ist eine technische Schutzmaßnahme sicher, und so war auch der CD-Kopierschutz recht schnell geknackt, und der Musiktausch im Internet ging weiter.

Um Anwender zusätzlich abzuschrecken, wurde umfangreich Werbung geschalten. Einige Schauprozesse, in denen die 'dicken Fische der Szene' verhaftet und eingesperrt wurden, verunsicherten die Anwender. Doch viele tauschten weiter Musik, vor allem weil sie sonst keine Möglichkeit hatten, ihre MP3-Player mit der aktuellen Musik zu füllen. Denn Kopieren der Musik von CDs (das s.g. rippen) war kaum noch möglich.

Gerade durch die große Verbreitung des MP3-Formats mussten die Musikkonzerne reagieren. Es wurden legale Musikportale geschaffen, in denen man sich legal (für meist 1EUR pro Lied) Musik online auf seinen PC laden und diese dann auf CD brennen oder auf seinen MP3-Player kopieren kann. Doch halt, so leicht wollte man es dem Anwender dann doch nicht machen. Es wurde ein Verfahren entwickelt, mit dem der Anwender in der Art und Weise, wie er seine Musik nutzt, regelrecht beschränkt wird.

1.2 Der Begriff DRM

Digital Rights Management (digitale Rechteverwaltung), abgekürzt DRM, ist ein Verfahren mit dem Urheber- und Vermarktungsrechte an geistigem Eigentum, vor allem an Film- und Tonaufnahmen, aber auch an Software oder elektrischen Büchern im Computerzeitalter gewahrt, sowie Abrechnungsmöglichkeiten für Lizenzen und Rechte geschaffen werden. Befürworter argumentieren, dass mit DRM die bisherigen Zwangsabgaben auf z.B. Leerkassetten oder Fotokopierer an GEMA und VG Wort überflüssig werden, sowie Rechteinhabern und Benutzern neue Geschäftsmodelle wie die Vermietung oder die Nutzung nach Dauer, Häufigkeit oder Umfang eine gerechte Abrechnung ermöglichen. Kritiker warnen vor allem vor Datenschutzproblemen und möglichen Einschränkungen bei der Benutzerfreundlichkeit und fairen Nutzung.

Kapitel 2

Grundlegende Funktionsweise

2.1 verteilte softwarebasierte DRM-Systeme

DRM-Systeme schützen die elektronischen Waren meist per Verschlüsselung. Die zur Entschlüsselung und Wiedergabe nötige Software setzt gleichzeitig die Nutzungsregeln durch. So kann ein Anbieter beispielsweise technisch verhindern, dass ein heruntergeladenes Musikstück mehr als dreimal abgespielt wird - danach ist eine Nachlizensierung fällig.
Alle am Markt befindlichen DRM-Systeme setzten sich aus mehrern Komponenten zusammen. Diese können sein (aus ct 16/2002 Seite 182):

- Benutzeridentifizierung
- Verschlüsselung
- Kopiersperre
- Authentizitätsprüfung
- Nutzungsbedinungen (Metadaten)
- Kopierkontrolle
- Zugangskontrolle
- digitale Wasserzeichen
- digitale Fingerabdrücke
- manipulationssichere Hard- und Software
- Zahlungssystem

Die meisten DRM-Systeme lassen sich in 3 große Systeme unterteilen: Den Content-Vertrieb, das Clearinghouse und das Endgerät (Abb 2.1).
Dabei wird im Content-Vertrieb der Inhalt (also das digitalisierte Musikstück) in einen Container mit mehrschichtiger Hülle gesteckt. Dieser Container wird mit Metadaten versehen, die die Bedingungen und Kosten, unter denen sich der Inhalt lesen lässt, enthalten und in der s.g. 'Rights Expression Language' vorliegen. Diese Metadaten ermöglichen die automatische Kommunikation zwischen den DRM-Komponenten. Bisher hat der Container noch keinen Nutzerbezug, er wird nun in eine Datenbank gespeichert.
Bestellt ein Nutzer ein Musikstück, übernimmt das s.g. Clearinghouse die Schnittstelle zwischen Nutzer und Content-Vertrieb. Der Container wird mittels eines (i.d.R. asymmetrischen) Verschlüsselungsalgorithmus gesichert und erlaubt dem Nutzer den Zugang über einen speziellen Schlüssel. Der Content hat nun einen Nutzerbezug und wird an das Endgerät übermittelt.
Bei der ersten Wiedergabe baut der Client eine Verbindung zum Clearinghouse auf und gleicht die Nutzungsbedingungen ab. Die Datei wird danach für die ausgehandelten Bedingungen freigeschaltet. Dabei erfolg i.d.R. ein Abgleich zwischen allen drei Instanzen.

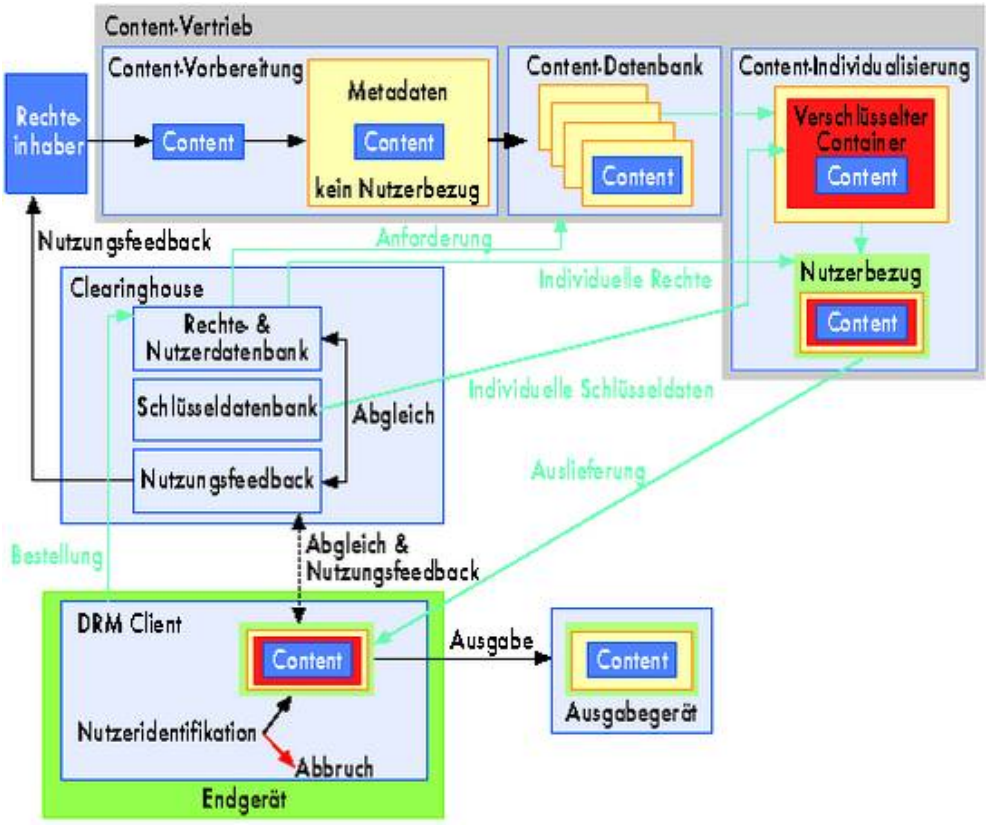

Abb 2.1: allgemeine Funktionsweise eines DRM-Systems

Jedes DRM geschützte Musikstück wird i.d.R. zusätzlich noch durch Wasserzeichen bzw. Fingerabdrücke markiert. Dies gibt den Rechteinhabern die Möglichkeit, bei Bruch des Kopierschutzes den Schuldigen ausfindig zu machen. Ein Wasserzeichen muss zwei Anforderungen genügen: ersten darf es die Qualität des Musikstückes nicht schmälern und zweitens muss es so robust sein, dass es ohne einen Qualitätsverlust nicht herausgelöst werden kann. Diese Wasserzeichen müssen sogar überleben, wenn das Stück über einen analogen Ausgang abgegriffen und anschließend wieder digitalisiert wurde.

2.2 hard- und softwarebasierte DRM-Systeme

Um die DRM-Systeme vor Missbrauch noch stärker zu schützen, versuchen die 'Großen' der Branche, allen voran Microsoft, Intel und IBM, von den reinen softwarebasierten DRM-Systeme wegzukommen und die kritischen Komponenten der DRM-Systeme (z.B. das Ver- und Entschlüsseln der Inhalte) in die Hardware zu verlagern. So schlossen sich viele nahmhafte Firmen zur s.g. TCG (Trusted Computing Group) zusammen, und entwickelten ber Jahre einen Chip, der die Computer revolutionieren soll. Dieser Chip ist bekannt unter dem Synonym TPM (Trusted Platform Module) und wird voraussichtlich bald in jedem handelsüblichen PC stecken. Intel stattet seine Prozessoren nach eigenen Aussagen schon mit diesen Modulen aus, lässt sie aber noch deaktiviert.
Ein entsprechendes Betriebssystem (z.B. Windows Vista - erscheint voraussichtlich nächstes Jahr) vorausgesetzt, lässt sich mit dieser Kombination jeder digitalisierte Inhalt sichern. Der Chip wacht darüber, ob Software ohne Lizenz genutzt, die Hardware verändert oder eine Datei ohne Erlaubnis geöffnet wird. Das TPM verschlüsselt ausserdem den Datenverkehr zwischen den Komponenten eines Systems mit einem 2048Bit-Schlüssel. Eben dieser Schlüssel (der auf jedem PC bzw TPM anders ist) kann dann auch die vom DRM-System verschlüsselte Audio-Datei entschlüsseln und zur Wiedergabe freigeben. Dabei kontrolliert der Chip sogar, ob die Wiedergabesoftware (z.B. der Windows Media Player) vertrauenswürdig ist.
Die Fantasien der Medienbranche gehen sogar so weit, dass nicht nur PCs, sondern jegliche elektronische Unterhaltungsgeräte ein solches TPM enthalten sollten. Das würde angeblich soweit führen, dass ein Camcorder im Kino das digitale Wasserzeichen des Films erkennt und die Aufnahme verweigert.

Kapitel 3

aktuelle DRM-Systeme

3.1 Windows Media DRM

Auch Microsoft hat die zunehmende Bedeutung von DRM bemerkt, und versucht, sich ein Stück vom 'DRM-Kuchen' abzuschneiden. Dabei benutzt MS hauseigene Mittel, zum Beispiel den Windows Media Player, der standardmäßig bei jedem Windows Betriebssystem dabei ist. Hinzu kommt das eigene Dateiformat 'Windows Media File' (wma für audio, wmv für video). Die Dateien sind verschlüsselt, damit man seine Musik am PC wiedergeben kann, benötigt man einen Key. Dieser wird vom 'Windows Media Rights Manager' verwaltet, über den der Urheber Zugriffsrechte vergeben kann.

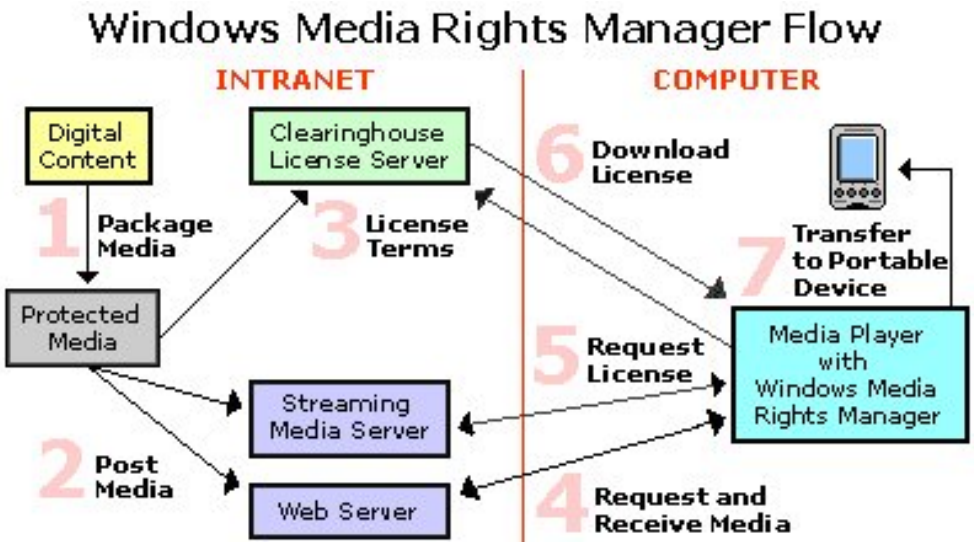

Abb 3.1: Windows Media DRM und der Windows Media Rights Manager

Die Funktionsweise des Windows Media Rights Managers sei hier kurz erklärt (Abb Abb 3.1):

1. Die Datei wird verpackt und verschlüsselt, zusätzliche Informationen können eingebunden werden.
2. Die (verschlüsselten) Dateien werden auf Servern bereitgestellt (streaming oder download).
3. Lizenz-Server wird eingerichtet. Dieses s.g. Clearinghouse verwaltet die Rechte des Urhebers.
4. Erwerb der Lizenz. Vom Clearinghouse wird ein Key gekauft, mit dem die verschlüsselte wm-Datei abgespielt werden kann.
5. Wiedergabe der Datei. Die Datei wird mit Hilfe des Keys entschlüsselt und kann nun wiedergegeben werden.

3.2 Apples FairPlay

iTunes Music Store (iTMS) bezeichnet das Online-Musikgeschäft der Firma Apple. Es wird dabei auf das AAC-Format und das DRM-System FairPlay gesetzt. Fairplay ist in die QuickTime-Technologie eingebunden. Jede Datei, die über den iTMS gekauft wird, ist mit diesem System fest verbunden und kann somit nur auf iPods geladen werden.
Ein im iTMS gekauftes Musikstück kann auf bis zu 5 Rechner wiedergegeben, beliebig viele iPods kopiert und beliebig oft gebrannt werden. Beim Brennen auf Audio-CDs geht der Kopierschutz verloren, sodass nach dem 'Rippen' der Musik ins DRM-freie MP3 oder WAV-Format eine freie Kopie der Musik auf dem Rechner vorliegt. Diese Freiheit hat allerdings einen Qualitätsverlust zur Folge, da die AAC-Dateien i.d.R. eine viel höhere Qualität als gängige Audio-CDs besitzen.
Der iTMS ist für MacOS X sowie Windows 2000 und XP erhältlich. Unter Linux ist es möglich, über den Emulator Wine die iTunes Software zu starten. Lieder können kostenlos 30sec. in voller Qualität probegehört werden. Der Preis für ein Stück beträgt 0.99, ein Album schlägt mit 9,99 zu Buche. Die Auswahl umfasst ca. 2Mio Titel.

3.3 OMA DRM Standard 2.0

Die Open Mobile Alliance ist eine Organisation bestehend aus ca 360 Unternehmen. Sie verfolgt u.a. die Ziele, den gesamten mobilen Markt zu erschlie-

ßen, eine nahtlose Anwendungsinteroperabilität und einen Wettbewerb auf Grundlage gemeinsamer Standards.
Für den mobilen Musik-Markt ist besonders der OMA DRM Standard 2.0 interessant. So soll es möglich sein, geschütze Inhalt (z.B. Musik) über Download, Stream oder über andere verbundene Geräte auf dem Mobiltelefon zu erhalten. Eine Vorschaufunktion und Kompatibilitätscheck ist integriert. Desweiteren soll es möglich sein, die geschützen Inhalt in andere DRM-Standards zu konvertieren, sodass man z.B. die über das Handy geladene Musik auch auf dem heimischen PC wiedergeben kann. Auch eine Weitergabe der Rechte ist mglich, um z.B. Musik als Geschenk zu kaufen. Sollte das Endgerät einmal gewechselt werden, ist eine Neuvergabe der Rechte möglich.

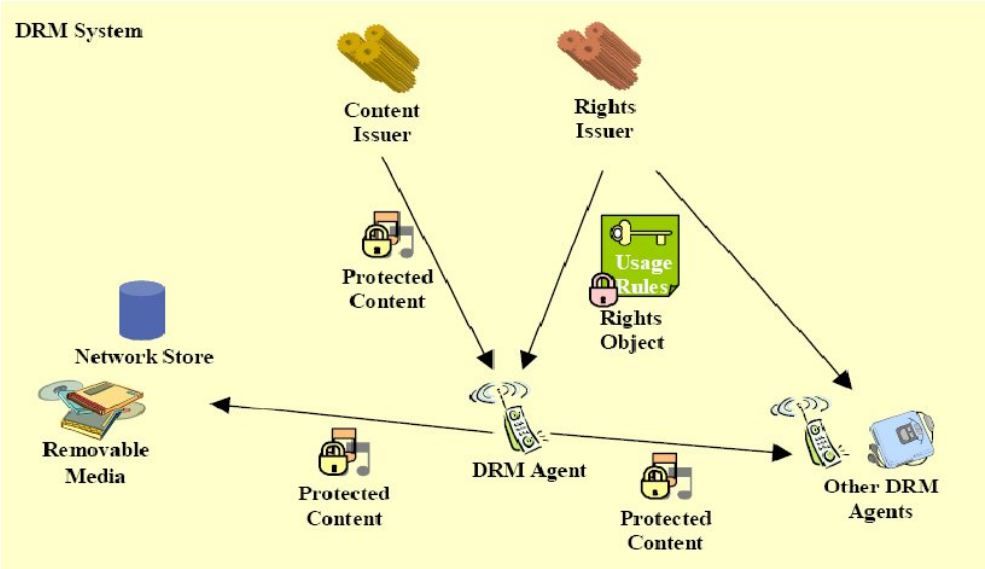

Abb 3.3: bersicht ber den OMA DRM-Standard 2.0

Der Inhalt ist vom Recht getrennt, so wie man das von DRM-Systemen gewohnt ist. Die Inhaltsdaten liegen binär vor, das Recht in der Rights Expression Language. Im DRM-Agent muss eine vertrauenswürdige Instanz enthalten sein, hier ist zum Beispiel ein TPM von Bedeutung. Der DRM-Agent gibt den Inhalt wieder und setzt auch gleichzeitig das Recht durch. Dieses Recht ist vom Aussteller digital signiert und somit gegen Manipulation geschützt. (Abb Abb 3.3)

Der OMA DRM Standard ist sehr umfangreich und komplex, es wurden bisher nur die Schnittstellen festgelegt, um einen ausreichenden Wettbewerb zu gewährleisten. Da der DRM-Agent die Einhaltung des Rechts übernimmt, ist die Sicherheit des Standards stark von diesem abhängig.

Kapitel 4

Fazit

4.1 Digital Restriction Management?

Aus Sicht des Nutzers birgt DRM nicht nur Nachteile. Obwohl er nun für jedes einzelne Lied Geld zahlen muss und teilweise die Nutzung des Erworbenen sehr eingeschränkt wird, kann er mit ruhigem Gewissen die Lieder aus dem Internet laden und sich anhören. Ausserdem hat er nun eine Garantie, dass die geladene Musik höchsten qualitativen Ansprüchen genügt und er seinen Teil dazu begetragen hat, dass die Künstler für ihre Werke bezahlt werden.
Viele Menschen, besonders in Amerika, denken zur Zeit um und setzen auf die 'Qualität aus einer Hand'-Marke. Apple verdient dadurch sehr viel Geld. Nicht nur durch den Verkauf der kleinen, hochwertigen iPods, sondern auch mit dem Verkauf von Musik über den firmeneigenen Online-Shop iTunes. Dazu trägt sicher auch bei, dass die von Apple gekaufte Musik den zur Zeit lockersten Umgang erlaubt.
Microsoft hat den Trend mal wieder verschlafen, und viel zu spät seinen eigenen Standard eingebracht. Da der MediaPlayer zur Zeit der einzige Player ist, der Microsofts WM-Dateien abspielen kann, und die meisten PC-Nutzer diesen (dank der quasi-Monopolstellung Microsofts im Betriebssystems-Sektor) schon auf ihrem Rechner haben, ist es allerdings für Microsoft nicht schwer, seinen Windows-Media-Standard neben der Apple-Konkurrenz zu platzieren.
Der OMA-DRM-Standard kann als Vorläufer gesehen werden. Durch den Einsatz der Trusted Platform Module ist ein Aushebeln des Kopierschutzes nahezu unmöglich. Sollte sich das System als praktikabel erweisen, steht dem Einzug der TPMs in den HeimPC oder andere Mediageräte nichts mehr im Weg.

4.2 Datenschutz

Ganz weit oben steht immer der Datenschutz. Ob und in welchem Ausmaß Firmen ein Nutzerprofil erstellen, bleibt wohl ein gut gehütetes Geheimnis. Klar ist jedoch: ein personalisierter Shop, der mir schon auf der Startseite sagt, welche Musik mir gefällt, ist nicht neu. Die Unterhaltungsbrache wird alles dafür tun, Ihre Musik geziehlt zu verkaufen. Und manchmal kann es doch auch ganz praktisch sein, wenn man von einem Computer auf ein Lied hingewiesen wird, von dem man noch nie etwas gehört hat, welches einem aber sehr gut gefällt. Auf diese Art und Weise werden dann beide Seiten glücklich: der Nutzer und der Verkäufer.

4.3 Quellenangaben

c't2002/16
c't2005/03
c't2005/05

http://www.microsoft.com/windows/windowsmedia/technologies/overview.aspx
http://de.wikipedia.org/wiki/Digital_Rights_Management
http://de.wikipedia.org/wiki/FairPlay
http://www.it-academy.cc/content/article_browse.php?ID=884
http://www.ldv.ei.tum.de/media/files/lehre/hauptseminar/ss2005/08_OMA%20DRM%20Standard%202.0.pdf