Ruhr-Universität Bochum
Lehrstuhl Kommunikationssicherheit
Seminar: IT-Sicherheit
Wintersemester 2003/2004

DRM-Systeme

Von: Kai Schmitz-Hofbauer
Matrikel-Nr.: 10898225116
Betreut durch: Dipl.-Soz.Wiss. Marcus Heitmann

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungen

AAC	Advanced Audio Coding
COM	Component Object Model
DRM	Digital Rights Management
eBook	electronic Book
EMMS	Electronic Media Management Services
MPEG	Moving Pictures Experts Group
PDF	Portable Document Format
P2P	Peer to Peer
SDK	Software Development Kit
WMA	Windows Media Audio
WMRM	Windows Media Rights Manager
WMV	Windows Media Video
XML	Extensible markup language

1 Einleitung

Das Internet ist in den letzten Jahren zu einem der wichtigsten Kommunikationsmedien geworden. Es ermöglicht einen einfachen Zugang zu digitalen Informationen jeglicher Art. Insbesondere P2P-Tauschbörsen haben in der jüngeren Vergangenheit an Beliebtheit gewonnen und verzeichnen einen ernormen Zuwachs. Die Tauschbörsen werden häufig dazu benutzt, sich einen kostenlosen Zugang zu urheberrechtlich geschützten digitalen Gütern wie zum Beispiel Musik, Filme oder eBooks zu verschaffen. Dies setzt die Rechteinhaber und Anbieter dieser Güter unter erheblichen Druck. Sie wollen die (sehr kostengünstige) technische Infrastruktur des Internet für den Vertrieb ihrer Produkte nutzen, zugleich aber die illegale Verbreitung der digitalen Güter durch Raubkopien verhindern. Die zu diesem Zweck eingesetzen Schutzmechanismen werden von den Anbietern als DRM *(Digital Rights Management)* bezeichnet. DRM hat die Aufgabe, die Nutzungsbedingungen des Anbieters bzw. des Rechteinhabers durchzusetzen. DRM legt die Bedingungen und Nutzungsbeschränkungen fest, unter denen Kunden digitale Güter wiedergeben dürfen. Diese treten in den verschiedensten Formen auf und gehen über einfachen Kopierschutz weit hinaus. So kann zum Beispiel der Anbieter von Dokumenten bestimmen, wer ein Dokument einsehen/abspielen kann, wie lange er es einsehen kann, wer es ändern darf oder ob und wie oft es kopiert werden darf. Häufig werden die Nutzungsberechtigungen für Dokumente auch an eine bestimmte Hardwarekonfiguration gebunden, so dass sich das Dokument nach einem Kopieren oder nach einer Änderung der Hardwarekonfiguration nicht mehr öffnen bzw. abspielen lässt. Diese zahlreichen Nutzungseinschränkungsmöglichkeiten sind der Grund dafür, warum Kritiker das Akronym DRM als *Digital Restrictons Management* auflösen.
Ziel dieser Seminararbeit ist es, die Funktionsweise, Vor- und Nachteile sowie der Grad des Schutzes von DRM-Systemen an Beispielen vorhandener DRM-Systeme aufzuzeigen und zu erläutern. Dabei wird schwerpunktmäßig der *Windows Media Rights Manager* thematisiert. Weitere DRM-Systeme sollen kurz angesprochen werden.

2 Mögliche Komponenten von DRM-Systemen

Ein DRM-System besteht aus mehreren Komponenten bzw. Elementen. Welche Komponenten in einem konkreten DRM-System zum Einsatz kommen, hängt maßgeblich von dem verwendeten DRM-System sowie vom Geschäftsmodell des Anbieters ab. Dieser Abschnitt beschäftigt sich damit, mögliche Komponenten von DRM-Systemen vorzustellen.

Eine Aufgabe von DRM-Systemen ist es, den Zugang und die Nutzung von digitalen Inhalten zu kontrollieren und dadurch den Nutzer zu veranlassen, für den Inhalt zu bezahlen (vgl. [uni-bern 03]). Die Identifizierung des Nutzers soll sicherstellen, dass nur Berechtigte auf den Inhalt zugreifen. Ein nutzungsbezogenes Abrechnungsverfahren muss darüber hinaus exakt feststellen können, welche Leistungen ein bestimmter Kunde in Anspruch genommen hat. Die Aufgabe der Benutzeridentifizierung übernimmt die Komponente **Benutzeridentifizierung**. Diese Identifikation kann über jedes beliebige Identifikationsverfahren erfolgen, wie zum Beispiel Angabe eines Benutzernamens und eines Passwortes. Viele DRM-Systeme verwenden zur Identifikation eindeutige Indentifizierungsnummern der zugrunde liegenden Endgeräte, wie zum Beispiel die Seriennummer eines mp3-Players oder eines eBook-Readers. Der Nachteil dieser Methode ist, dass die erworbenen Inhalte an dieses Gerät gebunden sind. Ein einmal erworbenes Musikstück ließe sich so entweder auf einem mp3-Player oder dem Heim-PC oder dem Laptop abspielen.

Verschlüsselung ist eine weitere wichtige Komponete eines DRM-Systemes. Bei dem Großteil der DRM-Systeme kommen asymmetrische Verschlüsselungsverfahren zum Einsatz. (vgl. auch im Folgenden [Günnewig 02]) In Verbindung mit einer digitalen Signatur sollen die **Authentizität und Integrität** der Inhalte zusätzlich geschützt werden. Die Verschlüsselung dient außerdem als **Zugriffsschutz** vor unberechtigtem Zugriff.

Die Komponente **Kopiersperre** sorgt dafür, dass digitale Inhalte nicht ohne Genehmigung kopiert werden können. Hier kommen diverse unterschiedliche Kopierschutzmechanismen zum Einsatz.

Oft ist es aber nur eine Frage der Zeit, bis ein solches Verfahren ausgehebelt wird. Falls es so weit gekommen ist, will ein Anbieter wissen, wer für die Verbreitung verantwortlich. Zu diesem Zweck können **digitale Wasserzeichen** eingesetzt werden. Ein digitales Wasserzeichen stellt ein transparentes nicht wahrnehmbares Muster dar, welches in das Datenmaterial eingebracht wird. Dieses Muster dient dazu, ent-

weder das Vorhandensein einer Kennzeichnung anzuzeigen oder Informationen zu codieren. Diese Informationen können Urheberinformationen und auch Kundeninformationen enthalten. Digitale Wasserzeichen bieten eine Möglichkeit, unerlaubtes Kopieren aufzuspüren, indem sie als unsichtbare Markierung dauerhaft zum Dokument gehören. Somit können Musikstücke, Texte und Bilder über die für den Urheberschutz relevanten Daten informieren. Aufgrund der versteckten Informationen kann genau nachvollzogen werden, wer wann unter welchen Bedingungen das Original kopiert hat. Digitale Wasserzeichen können somit die widerrechtliche Nutzung der digitalen Werke aufdecken.

Eine weitere mögliche Komponente eines DRM-Systemes sind **Suchsysteme**. Suchsysteme werden dazu eingesetzt, unberechtigte Kopien digitaler Inhalte zu finden. Lokalisiert die Suchmaschine einen entsprechenden Inhalt (zum Beispiel auf einem Webserver als Download-Angebot), so wird geprüft, ob dem Anbieter oder Nutzer des digitalen Inhaltes die erforderlichen Berechtigungen erteilt wurden. Suchsysteme werden oft in Verbindung mit digitalen Wasserzeichen eingesetzt (vgl. [uni-bern 03]).

Damit das DRM-System selbst nicht kompromittiert werden kann, muss es aus **manipulationssicherer Hard- und Software** bestehen. Dies bezieht sich auch auf die Abspielgeräte. Diese müssen insbesondere gegen Manipulationsversuche der Nutzer resistent sein. Sowohl die Hardware als auch die Software muss daher manipulationssicher ausgestaltet sein. Als mögliche Hardwarekomponenten seien an dieser Stelle der Vollständigkeit halber *Smartcards* oder *Dongles* erwähnt. Mögliche Softwarekomponenten können spezifische Player wie zum Beispiel der *Microsoft Media Player* oder *Real One* ein.

Um feststellen zu können, worum es sich bei einer gegebenen Datei handelt, werden ihr Informationen über den Inhalt, die Künstler und die Rechteinhaber beigefügt. Diese Informationen werden als **Metadaten** bezeichnet. Das Format dieser Daten ist im Idealfall standardisiert. Erst durch den Einsatz von Metadaten auf Basis eines standardisierten Formates ist eine automatische Kommunikation zwischen den DRM-Komponenten möglich.

DRM-Systeme werden meist in komplexe **E-Commerce-Systeme** integriert und so mit einem **Abrechungs- und Zahlungssystem** verknüpft. Nur so ist ein kommerzieller Vertrieb mit DRM-Unterstützung digitaler Güter überhaupt möglich. Die Kommunikation zwsichen dem DRM-System und E-Commerce-System erfolgt im Idealfall über standardisierte Schnittstellen.

Es sei noch einmal ausdrücklich betont, dass diese Auflistung nur eine Auswahl möglicher Komponenten bzw. Bestandteilen von DRM-Systemen darstellt. Welche Komponenten in einem konkreten DRM-System eingesetzt werden, hängt maßgeblich vom Geschäftsmodell des Anbieters ab.

3 Beispiele für DRM-Systeme

3.1 Windows Media Rights Manager

Für DRM hat Microsoft den *Windows Media Rights Manager* (WMRM) entwickelt, der eine Plattform für die sichere Distribution von digitalen Inhalten bereitstellen soll (vgl. auch im Folgenden [Microsoft 03-1]). Er ist das Kernstück von Microsofts DRM-Architektur. Er ist fester Bestandteil von *Microsoft Windows Media* und ist bereits in die aktuellen MS-Betriebssysteme integriert. Der *Microsoft Media Player* nutzt ebenfalls diese Technologie. Auf Grund der hohen Anzahl weltweit installierter *Windows*-Betriebssyteme und somit bereits vorhandener DRM-Infrastruktur kommt dem Windows Media Rights Manager eine große Bedeutung zu. Typische Einsatzgebiete des Windows Media Rights Managers sind Musik-Portale oder Online-Videotheken. Der Windows Media Rights Manager lässt sich nicht nur bei der Distribution von digitalen Inhalten über das Internet einsetzen, sondern es gibt ebenfalls Verwendungsmöglichkeiten bei CD-ROM oder DVD-ROM-basierten Anwendungsfällen. Solche Szenarien werden im Folgenden nicht weiter thematisiert. Zentrale Komponente des Windows Rights Managers ist eine Verschlüsselungkomponente, die nur autorisierten Benutzern Zugang zu den Medieninhalten gestattet. Möchte ein Benutzer eine verschlüsselte Mediendatei ansehen oder anhören, so muss er hierfür eine entsprechende Lizenz erwerben. Diese Lizenz enthält unter anderem einen Schlüssel. Mit Hilfe des Schlüssels kann die Datei entschlüsselt werden und der Inhalt entsprechend genutzt werden. Neben dem Schlüssel enthält die Lizenz auch Nutzungsbedingungen.
Bevor näher auf die Handhabung der Lizenzen eingegangen wird, wird zunächst die Funktionsweise des WMRM erläutert. Abbildung 1 zeigt, wie digitale Inhalte mit dem WMRM geschützt und vertrieben werden.
Zwischen *Verpacken und Verschlüsselung* der Medien-Datei bis hin zum *Abspielen* auf dem Abspielgerät des Kunden sind sieben Schritte notwendig. Diese Schritte sollen im Folgenden näher erläutert werden.

(1) Verpackung (*Packaging*) In einem ersten Schritt (in der Abbildung mit 1 gekenzeichnet) wird in einem Prozess, der auch als *packaging* bezeichnet wird, ein verschlüsseltes Paket des digitalen Gutes erstellt. Im Rahmen des *packaging*-Prozesses wird ebenfalls eine Lizenz erstellt, die den Schlüssel zum Entschlüsseln der Mediendatei enthält. Die Lizenz wird separat vertrieben. Neben dem verschlüs-

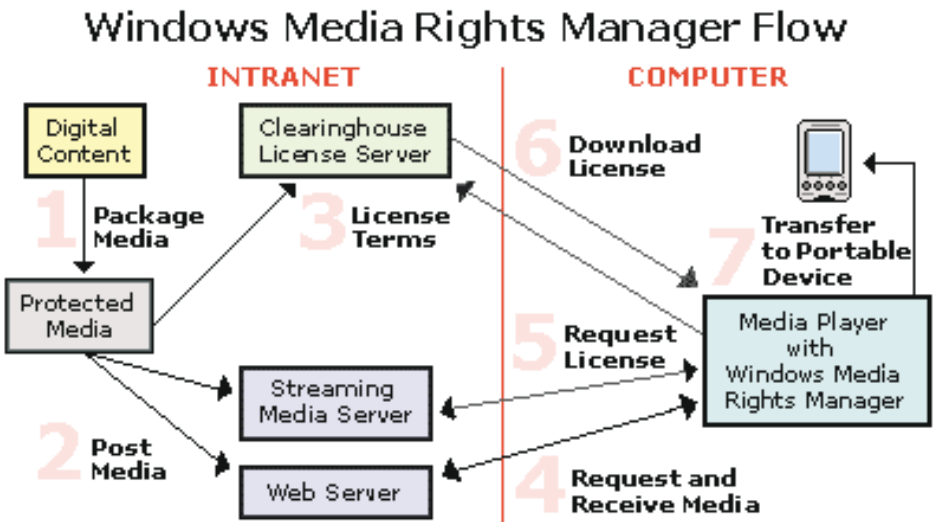

Abbildung 1: Funktionsweise des WMRM [Microsoft 03-1]

selten Inhalt wird das Paket um weitere Informationen ergänzt, wie zum Beispiel Eigentümer oder Informationen darüber, wo eine Lizenz für das digitale Gut erworben werden kann. Als Dateiformate kommen hier *Windows Media Audio* (WMA) und *Windows Media Video* (WMV) zum Einsatz.

(2) Distribution (*Distribution*) Der nachfolgende Schritt beschäftigt sich mit der Distribution des Paketes. Es bietet sich zum einen an, Mediendateien auf einem Webserver zum *download* anzubieten. Es ist aber auch möglich, die Daten per CD oder e-mail zu vertreiben.

(3) Server für Lizenzen einrichten (*License Terms*) Anschließend muss der Anbieter des digitalen Gutes einen *Clearinghouse License Server* (*Clearinghouse* = Verrrechnungsstelle) angeben, über den die entsprechende Lizenz inklusive Schlüssel für die geschützte Mediendatei bezogen werden kann. Die Hauptaufgabe des *Clearinghouse License Servers* besteht darin, die Lizenzanfragen des Konsumenten zu verifizieren. In diesem Schritt wird die Lizenz auf den benannten Server übertragen.

(4) Beschaffen der Mediendaten (*Request and Receive Media*) Der Nutzer verschafft sich in diesem Schritt Zugang zu den Medien. Dies kann entweder per *download* von einem Webserver oder durch Kontaktierung eines sog. *Streaming Media Servers* geschehen.

(5-6) Erwerb der Lizenz (*Request and Download License*) Beim Öffnen einer solchen Mediendatei erkennt der Media Player, dass die Daten durch WMRM geschützt sind und kontaktiert den in Schritt 1 angegebenen Lizenzserver (*Clearinghouse Server*). Der Vorgang wird automatisch gestartet, wenn der Nutzer versucht auf den geschützten Inhalt zuzugreifen. Die Lizenz kann automatisch ohne Benutzerinteraktion oder nach Angabe von Registrierungs- bzw. Abrechnungsdaten heruntergeladen werden.

(7) Abspielen der Mediendatei (*Playing the Media File*) In einem letzten Schritt kann die Mediendatei abgespielt werden. Dies kann entweder auf dem Heim-PC oder einem portablen Abspielgerät geschehen. Dazu benötigt der Nutzer allerdings ein Abspielgerät, das den *Windows Media Rights Manager* unterstützt. Beim Abspielen sind natürlich die in der Lizenz festgelegten Nutzungsbedingungen zu beachten.

Der Windows Media Rights Manager ist selbst kein eigenständiges Programm mit direkter Benutzer-Interaktion. Er besteht aus einem Satz von COM-Komponenten, die Softwareentwickler in ihre Anwendungen einbinden können. Hierzu steht das WMRM Software Development Kit (SDK) zur Verfügung. Eine detaillierte Betrachtung des WMRM SDKs würde den Rahmen dieser Seminararbeit sprengen. Es sei an dieser Stelle auf [Microsoft 03-2] und [Microsoft 03-3] verwiesen.

Im Folgenden soll nun thematisiert werden, wie Schlüssel- und Lizenzgenerierung beim Windows Media Rights Manager funktioniert. Abbildung 2 veranschaulicht diesen Sachverhalt. Wie bereits angesprochen, wird zum Abspielen einer verschlüsselten Mediendatei eine Lizenz benötigt, die den Schlüssel zum Entschlüsseln der Mediendatei enthält. Der Schlüssel setzt sich aus einer *License Key Seed* und einer *Key ID* zusammen. Die Key ID wird vom Rechteinhaber für jedes Werk vergeben. Sie ist auch in jeder verschlüsselten Datei enthalten. Bei der License Key Seed handelt es sich um einen (geheimen) Wert, der nur dem Rechteinhaber und dem Lizenzserver bekannt ist. Wenn eine Lizenz für eine verschlüsselte Mediendatei erzeugt wird, wird der Schlüssel mit Hilfe der Key ID und der License Key Seed bestimmt . Der Schlüssel wird anschließend in die Lizenz eingebettet. Nachfolgend wird die Lizenz auf den Rechner des Kunden übertragen. Mit Hilfe des Schlüssels aus der Lizenz kann die Mediendatei entschlüsselt und anschließend abgespielt werden. In der Lizenz sind

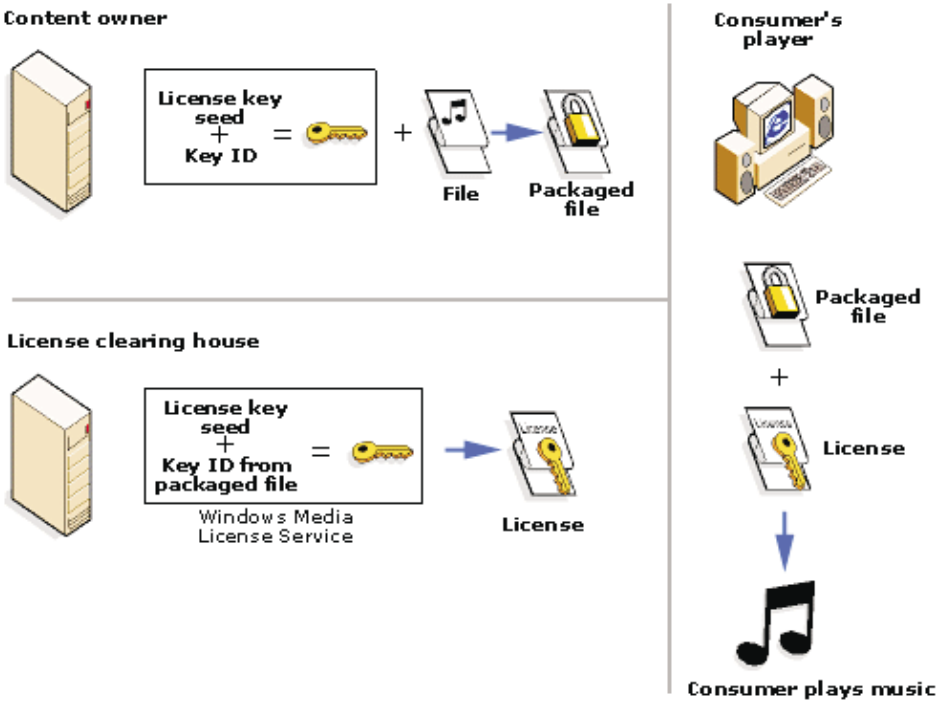

Abbildung 2: Lizenzen und Schlüssel [Microsoft 03-1]

ebenfalls die Nutzungsrechte für das Werk enthalten. Typische Nutzungsrechte beim WMRM sind:

- wie oft eine Datei abgespielt werden kann,
- auf welche Abspielgeräte eine Mediendatei übertragen und abgespielt werden darf,
- in welchem Zeitraum die Datei abgespielt werden darf (zum Beispiel Startzeitpunkt und Ablaufdatum),
- ob und wie oft ein Werk auf eine CD gebrannt werden darf,
- ob und wie oft der Benutzer Lizenzen sichern und wieder herstellen darf,
- auf dem Client benötigte *security level*, um die Datei abspielen zu dürfen.

Große Plattenfirmen wie EMI, BMG, Warner Music Group, Sony Music Entertainment und Universal Music Group nutzen den WMRM.
Das Muskiportal *Musicload* (vgl. [musicload 03]) von T-Online nutzt ebenfalls den WMRM. Dieses Portal stellt einen kostenpflichtigen download von WMA-Mediendateien

zur Verfügung. Abbildung 3 zeigt das Angebot eines Titels bei Musicload.

Abbildung 3: Musikportal Musicload [musicload 03]

Hier sind klar die (eingeschränkten) Nutzungsrechte zu erkennen. Das Werk lässt sich nach Kauf und downlaod unbegrenzt oft abspielen, aber nur dreimal auf CD brennen und auch nur dreimal auf portable Abspielgeräte übertragen.

3.2 Intertrust Rights|System

Ein weiterer großer Anbieter für DRM-Technologien ist Intertrust (vgl. auch im Folgenden [intertrust 03]). Intertrust vertreibt das DRM-System *Intertrust Rights|System*. Dieses System eignet sich zur Schutz jeglicher Art von digitalen Gütern von Audio- und Video-Dokumenten bis hin zu Textdokumenten. Dieses System weist viele Gemeinsamkeiten, aber auch einige Unterschiede mit dem im vorangegangenen Abschnitt vorgestellten Windows Media Rights Manager auf. Abbildung 4 gibt einen Überblick über Intertrust Rights|System. Im Folgenden soll nun die Funktionsweise dieser DRM-Lösung kurz vorgestellt werden. Das Produkt wurde so entworfen, dass es sich leicht in die technische Infrastruktur des Kunden integrieren lässt. Aus diesem Grund kommen auch offene Standards wie zum Beispiel XML und Java zum Einsatz. Das Rights|System lässt sich grob in vier Produktlinien unterteilen, nämlich **Packager**, **Server**, **Clients** und (optional) ein Software Development Kit **SDK**, um das Rights|System an die eigenen Gegebenheiten anzupassen. Diese Komponenten sollen nun kurz vorgestellt werden.

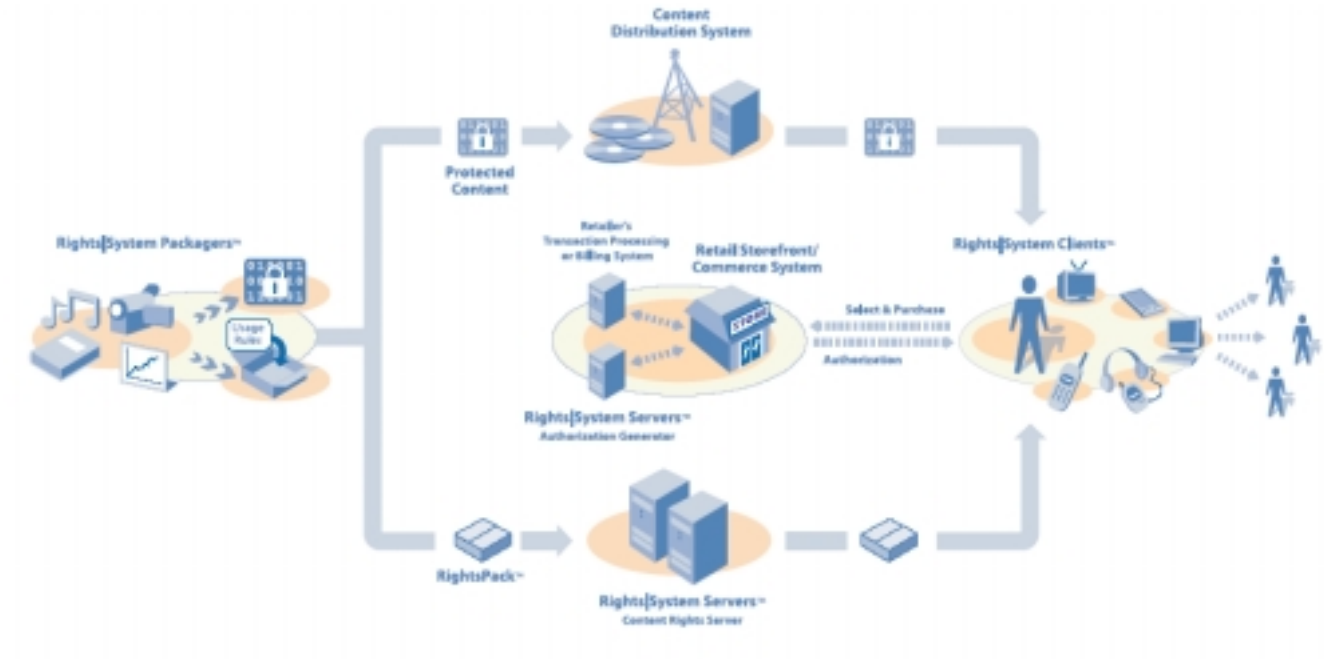

Abbildung 4: Intertrust Rights|System [intertrust 03]

Packagers Genau wie beim WMRM ist diese Komponente für das Verpacken und Verschlüsseln der digitalen Inhalte zuständig. Welche Aktivitäten genau in diesem Vorgang durchgeführt werden und welche Nutzungsbedingungen vergeben werden sollen, wird in einer XML-Beschreibung festgelegt, die dem Packager als Eingabe dient. Neben der Datei, die den verschlüsselten Inhalt enthält, generiert der Packager einen sogenannten **RightsPack** für jede Datei. Die Funktion des RightsPacks entspricht der der Lizenzen beim WMRM. Der verschlüsselte Inhalt kann auf den üblichen Wegen vertrieben werden. Die RightsPack-Datei wird auf einem sogenannten *Content Rights Server* platziert, dessen Funktion der eines Lizenzservers im Modell des WMRMs entspricht. Der Standard-Packager unterstützt gebräuchliche Dateiformate wie zum Beispiel MP3, AAC, MPEG4 oder PDF. Es ist aber auch möglich, den Packager über einen Plugin-Mechanismus um weitere Dateiformate zu erweitern. Zu erwähnen ist noch, dass der Packer zum einen als Einzelanwendung lauffähig ist, zum anderen aber auch integrierbar in Fremdsysteme ist.

Servers Die Serverprodukte des Rights|System basieren auf der Java Servlet Technologie und sind somit nicht an spezielle Plattformen gebunden. Dies ist ein deutlicher Unterschied zu der Lösung von Microsoft. Neben dem bereits erwähnten *Content Rights Server* gehört zu dieser Gruppe unter anderem auch der *Authorizati-*

on Generator, der grundlegende Autorisationsdienste zur Verfügung stellt. Diese Dienste können unter anderem von evtl. involvierten e-Commerce-Systemen genutzt werden.

Clients Für das Rights|System existiert Clientsoftware für verschiedene Plattformen und Geräte. Als Beispiel lassen sich *Rights|Desktop* für PCs, *Rights|PD* für portable Endgeräte, *Rights|Phone* für Mobilfunkgeräte und *Rights|TV* für TV-Boxen nennen. Allerdings sind diese Systeme nicht kompatibel mit dem Windows Media Rights Manager bzw. dem Windows Media Player. So müssen (Windows-) Anwender auf jeden Fall neue Software auf ihrem Computer installieren.

SDKs Intertrust stellt eine Reihe von Software Development Toolkits zur Verfügung, die es Softwareentwicklern erlauben, DRM-Mechanismen von Intertrust in ihre Anwendungen einzubinden bzw. das DRM-System an festdefinierten Stellen über Plugin-Mechanismen zu erweitern. Intertrust bietet verschiedene SDKs an, wie zum Beispiel *Rights|Audio* für Musicplayer, *Rights|Video* für Videoplayer, *Rights|Desktop* um die Benutzungsoberfläche des PCs anzupassen und das *Packager SDK* um den Packager an geeigneten Stellen zu erweitern.

Auch Intertrust kooperiert mit vielen großen Firmen. Lizenzpartner sind unter anderem Digital World Services (DWS), das DRM-Unternehmen der Bertelsmann AG, und die Sony Corporation. Um zu unterstreichen, wie vertrauenswürdig Intertrust ist, wird auf der Firmenwebseite damit geworben, dass zahlreiche Patente in Firmenbesitz sind. Um welche Patente es sich dabei konkret handelt und welchen Nutzen und Vorteil der Besitz dieser Patente für Kunden bzw. Anwender haben kann, wird auf der Intertrust-Seite selbst nicht erläutert. Es ist lediglich möglich, die Einträge für diese Patente aus einem Verzeichnisdienst für US-Patente abzurufen.

3.3 Weitere DRM-Lösungen

IBM bietet ebenfalls eine DRM-Lösung an. IBM vertreibt derzeit das DRM-System *Electronic Media Management Services* (EMMS). Dieses System eignet sich zum Schutz jeglicher Art von digitalen Gütern und ist nicht auf Audio und Video beschränkt. Um eine möglichst flexible Anwendung zu ermöglichen, setzt IBM bei EMMS ebenfalls auf offene Standards wie XML und Java. Der Integration in vorhandene IT-Infrastrukturen kommt in diesem System hohe Bedeutung zu. Aus die-

sem Grund setzt IBM auch auf Kompatibilität zum Windows Media Player. Dieses System kommt in Japan sehr häufig zum Einsatz. Da eine detaillierte Diskussion des Systemes den Rahmen dieser Seminararbeit sprengen würde, sei hier nur auf [IBM 03] verwiesen.
Auch Real Networks verfügt über eine eigene DRM-Plattform. Unter dem Namen *Real One* verstecken sich sowohl der Player für Musik und Video als auch eine Plattform für digitale Inhalte. Der RealOnePlayer bietet einen Plugin-Mechanismus, über den anderen Anbietern die Möglichkeit gegeben wird, ihre DRM-Schutzmechanismen in den Real Player zu integrieren. Real Networks stellt auch selbst Media-Dienste (*RealMedia*) zur Verfügung. Diese sind aber nur US-Kunden zugänglich. Eine detaillierte Betrachtung dieser Thematik erfolgt unter [RealNetworks 03] und [Hauser 03].
Adobe bietet ebenfalls eine DRM-Lösung an, den *Adobe Content-Server*. Dieses Produkt konzentriert sich schwerpunktmäßig auf den elektronischen Vertrieb von eBooks und PDF-Dokumenten. Bei PDF-Dokumenten sind die Nutzungsbedingungen in der Regel im Dokument selbst enthalten. Somit entfällt die Notwendigkeit einer separaten Lizenz. Typische Nutzungsbeschränkungen bei PDF-Dokumenten sind :

- Anzahl der Seiten, die betrachtet werden dürfen
- ob das Dokument gedruckt werden darf
- ob Teile des Dokumentes in die Zwischenablage des Betriebssystemes kopiert werden dürfen
- wie lange das Dokumente betrachtet werden darf

Auch an dieser Stelle sei nur auf [Adobe 03] verwiesen.

4 Schwächen von DRM-Schutzmechanismen

Die potentiellen Möglichkeiten von DRM-Systeme könnten bei Rechteinhabern und Anbietern von digitalen Gütern den Eindruck erwecken, als handele es sich bei DRM um eine Lösung, die sämtliche Probleme, die auf Urheberrechtsverletzungen basieren, auf einen Schlag lösen kann. Diese utopische Vorstellung wird von den Anbietern von DRM-Systemen gefördert. In der Realität weisen DRM-Schutzmechanismen heutiger DRM-Systeme einige Schwächen auf. In diesem Abschnitt sollen vergangene und gegenwärtige Schwächen der vorgestellten DRM-Systeme vorgestellt werden. Dabei wird sowohl auf spezifische Schwächen der einzelnen DRM-Systeme als auch auf Umgehungsmöglichkeiten für DRM-Schutzmechanismen eingegangen, die nicht an ein konkretes DRM-System gebunden sind.

Auf Grund des hohen Verbreitungsgrades ist gerade der *Windows Media Rights Manager* immer wieder Kompromittierungsversuchen ausgesetzt (vgl. auch im Folgenden [Wenz 03]). Einige dieser Versuche waren in der Vergangenheit erfolgreich. Bereits bei einer der ersten Versionen des WMRM (DRM1) konnten geschützte Musikstücke (im WMA-Format) mit Hilfe des Programmes **unfuck.exe** in uneingeschränkte WMA-Dateien konvertiert werden. Auch wenn DRM1 technisch bereits überholt ist, wird diese Version immer noch eingesetzt. Laut [Wenz 03] hat die Band *Bon Jovi* vor kurzem noch eine mit dieser Technologie geschützte Live-Aufnahme veröffentlicht, die die Käufer des letzten Albums von der Homepage der Band herunterladen konnten. Das Programm selbst sowie weitere Informationen können über [unfuck.exe] bezogen werden. Auch die Nachfolgerversion von DRM1 (DRM2) wurde von erfolgreichen Angriffen nicht verschont. Mit Hilfe des Programmes **FreeMe** können die Beschränkungen von mit DRM-geschützten Audiodaten im Format *Windows Media 7* ausgehebelt werden. Das Programm klingt sich dazu direkt in Microsofts DRM-System ein und nutzt bereits vorhandene Wiedergabelizenzen zur Verrichtung der Arbeit. Somit muss auf dem Rechner, auf dem FreeMe aufgerufen wird, bereits eine vorhandene Wiedergabelizenz vorliegen. Nach dem Aufruf von FreeMe kann die Datei dann aber ohne Einschränkungen verbreitet werden. Abbildung 5 veranschaulicht die Funktionsweise von FreeMe. Für FreeMe hat Microsoft schon vor einiger Zeit einen Patch herausgegeben. Bei Anbietern, die diesen Patch bereits eingespielt haben, bleibt FreeMe ohne Wirkung. Die Entschlüsselung der Dateien schlägt in diesem Fall mit der Meldung, der 'Content Key' sei zu lang, fehl. Auch wenn die beiden vorgestellen Werkzeuge bei der aktuellen DRM-Technologie von Microsoft

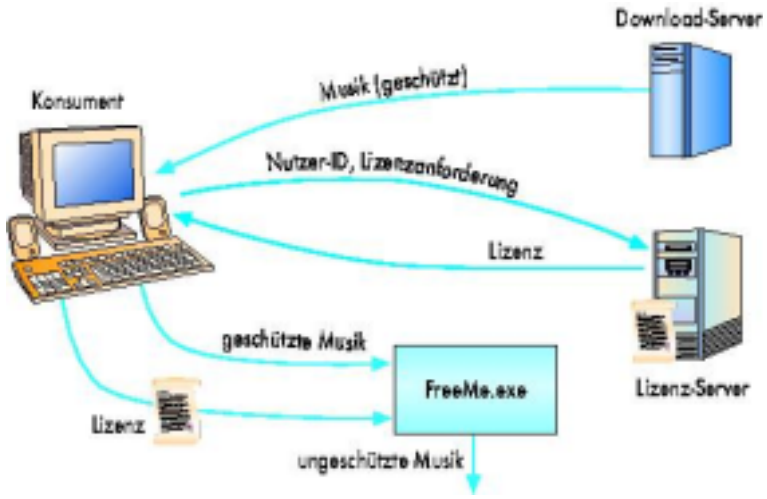

Abbildung 5: Das Programm FreeMe [Gleich 01]

ohne Wirkung bleiben, zeigen diese Beispiele, wie anfällig die Schutzmechanismen in der Vergangenheit waren. Bis die Schutzmechanismen der aktuellen Version überwunden werden, ist es wahrscheinlich nur eine Frage der Zeit.

Nicht nur die Schutzmechanismen von Microsoft wurden überwunden. Auch von Adobe geschützte eBooks und PDF-Dokumente konnten in der Vergangenheit von ihrem Schutz befreit werden (vgl. [Hauser 03]). Mit Hilfe des Programmes **Advanced Password Recovery** der russischen Firma Elcomsoft ist es möglich, die in einer PDF-Datei hinterlegten DRM-Nutzungsbeschränkungen zu deaktivieren. Außerdem ist es möglich, passwortgeschützte Dokumente zu öffnen. Zur Entschlüsselung verwendet das Programm sowohl Lexika- als auch *Bruteforce*-Angriffe. Dies wird insbesondere dadurch ermöglicht, dass bis zu einer PDF-Version von 1.3 (Acrobat 4) das PDF-Format eine Schlüssellänge von 40 Bit vorsieht . Laut [Hauser 03] war dieses Werkzeug mit Tests an digitalen Büchern, wie sie in Heft-CDs beiliegen, erfolgreich. Es ließen sich Nutzungsbeschränkungen so ändern, dass sich die Bücher beliebig lang lesen oder auch ausdrucken ließen.

Um DRM-Schutzmechanismen zu umgehen, ist es nicht zwingend notwendig, auf solche *Hackerprogramme* zurückzugreifen. Bei Audiodokumenten ist es zum Beispiel möglich, die Audiosignale am analogen Ausgang der Soundkarte abzufangen und aufzuzeichen. Dieses Vorgehen ist natürlich mit einem Qualitätsverlust verbunden. Viele Soundkarten haben einen digitalen Ausgang, an dem die Daten ohne Qualitätsverlust abgefangen werden können. Allerdings schließen viele Hersteller von Soundkarten den digitalen Ausgang bei der Wiedergabe DRM-geschützter Medien,

so auch die Soundkarte *Soundblaster Live*. Ein etwas anderer Ansatz macht sich den Umstand zunutze, dass geschützte Audiodaten auf dem Weg zur Soundkarte zwangsläufig entschlüsselt werden müssen. Ansonsten wäre eine Wiedergabe unmöglich. So ist es möglich, die Daten auf dem Weg zur Soundkarte abzufangen und die Ausgabe in eine Datei umzuleiten. Werkzeuge wie **Total Recorder** und **Virtual Audio Cable** für Windows-Systeme (vgl. [Total Recorder] und [Virtual Audio Cable]) oder **vsound** (vgl. [vsound]) für Linux richten im System eine virtuelle Soundkarte ein. Diese wird im System als Standardkarte registriert. Sämtlich Audiodaten werden dann an diese virtuelle Soundkarte weitergeleitet. Auf Wunsch schreiben diese Art von Werkzeuge die abgefangenen Daten in eine Datei, und zwar ohne jegliche Art von Einschränkungen. Da es sich dabei auch um digitale Daten handelt, kommt es zu keinem Qualitätsverlust. Für die Rechteinhaber und Anbieter von digitalen Audiogütern wird es nur schwer möglich sein, sich gegen diese Art von Umgehungsversuchen von DRM-Schutzmechanismen ernsthaft zu schützen.

Es muss auch die zeitliche Komponente berücksichtigt werden. Schlüssellängen, die heute noch genug Sicherheit bieten, tun dies in einigen Jahren oder Jahrzehnten, wenn neue Rechnergenerationen auf dem Markt sind, nicht mehr, so dass eine heute noch sicher verschlüsselte Datei dann ohne größere Probleme entschlüsselt werden kann.

Die hier aufgeführten Schwächen sind nur einige Beispiele für einen nicht wirkungsvollen Schutz der eingesetzten DRM-Systeme. Es lassen sich in der Praxis zahlreiche weitere Beispiele finden. Die hier aufgeführten Szenarien zeigen aber, dass DRM-Systeme keine Allheilmittel für Rechteinhaber und Anbieter von digitalen Gütern sind.

5 Fazit

DRM-Systeme haben für Rechteinhaber und Anbieter von digitalen Gütern viele Vorteile. DRM-Systeme ermöglichen Zugangs- und Nutzungskontrolle digitaler Medien, gewährleisten die Authentizität und Integrität digitaler Inhalte und ermöglichen ein automatisiertes Rechtemanagement. DRM-Systeme ermöglichen es, die kostengünstige technische Infrastruktur des Internet für den Vertrieb elektronischer Güter zu nutzen, zu gleich aber die illegale Verbreitung durch Raubkopien einzuschränken. Wie das vorangegangene Kapitel gezeigt hat, konnten die Sicherheitserwartungen in der Vergangenheit nicht hundertprozentig erfüllt werden. Neben den bereits diskutierten Schwächen haben DRM-Systeme viele weitere Nachteile. DRM-Systeme sind meist in sich abgeschlossene Systeme. Da Standardisierung in diesem Bereich noch nicht so weit fortgeschritten ist, sind viele Lösungen zueinander nicht kompatibel. Dies kann sich als einführungshemmend für einzelne Lösungen herausstellen. Kunden bzw. Nutzer von digitalen Medien müssen beim Kauf oft persönliche Daten hinterlassen. Bei den aktuellen Musikportalen müssen sich die Nutzer anmelden, wenn sie das kostenpflichtige download-Angebot nutzen wollen, beim Kauf einer CD oder einer DVD in einem Geschäft entfällt dies. Dieser Umstand birgt ein hohes Risiko von Verletzungen des Datenschutzes und der Privatsphäre. DRM-Systeme konzentrieren sich vorwiegend auf technische Sachverhalte. Ein effektiver Schutz kann nicht nur durch technologische Lösungen erfolgen. Hier müssen mehrere Faktoren zusammenwirken. Neben technischen Aspekten sind auch wirtschaftliche, soziale und vor allem rechtliche Gesichtspunkte zu beachten. Weiterhin stellt sich die Frage, ob die Schutzmechanismen derzeitiger DRM-Systeme nicht zu weit gehen. Ziel des Urheberrechtes war es nie, jedes Exemplar eines urheberrechtlich geschützten Stücks einzeln zu erfassen, zu registrieren und zu verrechnen. Ganz wichtig bei DRM-Systemen ist die zeitliche Komponente. Güter, die man einmal erworben hat, sollen auch nach Jahren oder Jahrzehnten noch wiedergegeben werden können. Was nützt es, wenn man für ein Audio-Musikstück unbegrenzte Abspielrechte erworben hat, das verwendete Dateiformat aber in zwanzig Jahren von Abspielgeräten nicht mehr unterstützt wird. Die wichtigste Komponente eines DRM-Systems wird meist nicht beachtet, nämlich der Kunde. Für die Nutzung der digitalen Güter muss er zahlreiche Einschränkungen akzeptieren, die ihm per DRM aufgezwungen werden. Inwieweit DRM-Syteme vom Markt akzeptiert werden und inwieweit sie sich durchsetzen werden, wird die Zukunft zeigen.

Literatur

[Adobe 03]

Adobe (2003): Content Server, http://www.adobe.com/products/contentserver/main.html am 5.12.2003

[Gleich 01]

Gleich, Clemens (2002): Entfesselte Musik - Microsofts neues Digital Rights Management ausgehebelt, in: ct 23/2002, S. 62-63

[Günnewig 02]

Günnewig, Dirk et. al (2002): Musik im Hochsicherheitstrakt: Digital Rights Management - Stand der Dinge, in: ct, 16/2002, S. 182-185

[Hauser 03]

Hauser, Tobias (2003): Finger weg: DRM-Systeme in der Praxis, in: ct 06/2003, S. 234-237

[IBM 03]

IBM (2003): IBM Electronic Media Management System, http://www-306.ibm.com/software/data/emms am 17.12.2003

[intertrust 03]

Intertrust (2003): Understanding DRMS Systems - An IDC White Paper, http://www.intertrust.com/main/research/whitepapers/IDC-UnderstandingDRMSystems.pdf am 8.12.2003

[Microsoft 03-1]

Microsoft (2003): DRM-Informationsseiten, http://www.microsoft.com/windows/windowsmedia/drm.aspx am 20.11.2003

[Microsoft 03-2]

Microsoft (2003): Windows Media Rights Manager SDK, http://www.microsoft.com/windows/windowsmedia/9series/sdk.aspx am 21.11.2003

[Microsoft 03-3]

Microsoft (2003): MSDN-Artikel - Windows Media Programming Guide, http://msdn.microsoft.com/library/default.asp?url=/library/-en-us/wmrm/htm/wmrm_sdk_guide_tymb.asp am 12.12. 2003

[musicload 03]

T-Online (2003): Musikportal Musicload, http://www.musicload.de am 30.11.2003

[RealNetworks 03]

Real Networks (2003): DRM-Informationsseiten von Real Networks, http://www.realnetworks.com/products/drm/index.html am 16.12.2003

[Total Recorder]

High Criteria(2003): Audiorekorder Total Recorder, http://www.high-criteria.com am 20.12.2003

[unfuck.exe]

Unfuck (2003): Das Programm unfuck.exe, http://go.to/unfuck am 20.12.2003

[uni-bern 03]

Universität Bern (2003): DRM-Informationsseiten des Institutes für Wirtschaftsinformatik - Abteilung Information Engineering der Universität Bern, http://www.ie.iwi.unibe.ch/forschung/drm am 14.11.2003

[Virtual Audio Cable]

NTONYX (2003): Audiorekorder Virtual Audio Cable, http://www.nt-onyx.com/vac.html am 20.12.2003

[vsound]

Erik de Castro Lopo (2002): Audiorekorder vsound für Linux, http://www.zipworld.com.au/%7Eerikd/vsound/ am 20.12.2003

[Wenz 03]

Wenz, Christian (2003): Ohren auf den Schienen - Umgehungsmöglichkeiten für DRM-Schutzmechanismen, in: ct 06/2003, S. 238-239