Digital Rights Management - Technik die begeistert?

Eine kritische Würdigung (nicht nur)
unter dem Aspekt der Systemsicherheit

Thilo Stadelmann
Matrikel-Nr. xyzabc

7. Juni 2003

Seminararbeit im Schwerpunkt TWA des Fachbereichs MNI der FH Giessen-Friedberg
im Sommersemester 2003 bei Prof. Dr. V. Klement / Prof. Dr. P. Kneisel

Inhaltsverzeichnis

Zusammenfassung

Diese Arbeit möchte einen Überblick über die generellen Techniken moderner DRM-Systeme unter dem Aspekt “Schutz & Sicherheit” vermitteln. Zu diesem Zweck wird ein allgemeines Schema zur Low-Level-Funktionalität erstellt und erläutert. Dem gegenüber wird auch auf weiter von dieser Ebene abstrahierende Ansätze eingegangen. Der Leser soll so in die Lage versetzt werden, aktuelle und künftige Systeme verstehen und bewerten zu können. Um die Relevanz und das Konfliktpotential des Themas voll erfassen zu können, wird zuvor auf nichttechnische Aspekte des DRM als Katalysator für gesellschaftliche Entwicklungen eingegangen werden. Gegen Ende werden die Ergebnisse der Teilaspekte zusammengeführt und bewertet sowie ein Ausblick auf die Zukunft gewagt.

1 Einführung

1.1 Motivation und Zielsetzung

Digital Rights Management (DRM) ist in aller Munde. Betrachtet man das große deutsche Computerfachblatt "c't" als Stimmungsbarometer für die Wünsche, Bedürfnisse und auch Ängste der IT-Branche, so impliziert allein die Anzahl der dort in den letzten Monaten zu diesem Thema erschienenen Berichte und Kommentare [1]-[22], dass es sich bei dem Phänomen DRM um etwas – wie auch immer geartetes – Großes handeln muss.

Und während der Markt in diesem Bereich fast ebenso schnell wächst wie die Anzahl jener Artikel, entstehen zu jedem neuen Produkt enthusiastische Produktbeschreibungen, in welchen die Marketingabteilungen immer neue Funktionalitäten und höhere Sicherheit versprechen.

Allerdings kratzen diese "Whitepapers" und deren Verarbeitung durch die populäre Presse meist nur an der Oberfläche dessen, *was* in diesen Systemen wirklich passiert. Und vor allem ist wenig darüber bekannt, *wie* dieses passiert.

Diese Arbeit möchte *keinen* Überblick über die am Markt etablierten Systeme mit deren speziellen Lösungen produktspezifischer Probleme geben. Auch soll nicht explizit auf einzelne Systeme eingegangen werden, um deren spezielle Funktionsweise, Handhabung oder korrespondierende Vermarktungsstrategie für digitale Inhalte zu erläutern.

Vielmehr ist es Ziel dieser Arbeit, die zugrunde liegenden Gemeinsamkeiten der vielen konkurrierenden, proprietären Systeme sowie die allgemeinen Schlüsseltechnologien und deren Komposition zu einem übergeordneten Ganzen aufzuzeigen. Der Fokus soll hierbei auf den Sicherheits-Funktionen des DRM liegen, da mit ihnen als Rückgrat des gesamten Systems dessen Ansinnen stehen oder fallen wird. Die Funktionen der darüber liegenden Schichten bieten eher softwaretechnisch-organisatorische Herausforderungen und sollen in einem eigenen Abschnitt kurz erläutert werden.

Gleichzeitig soll aber nicht die Illusion erzeugt werden, mit dem Verständnis der Technik allein könne das generelle Problem der Behandlung geistigen Eigentums im Zeitalter verlustfreier digitaler Kopien gelöst werden. Deshalb soll zu Anfang der geisteswissenschaftliche Rahmen abgesteckt werden, in welchem sich die Ingenieurs-Disziplinen betätigen mögen.

Zum Abschluss soll, neben einer finalen Kanalisation und Bewertung der genannten Fakten, ein etwas anderer Ansatz vorgestellt werden: Als Alternative zu der hier vorgestellten Klasse von Systemen hat der Light-Weight-DRM-Ansatz, welcher momentan am Fraunhofer Institut für Integrierte Schaltungen entwickelt wird, einiges Potential, die Zukunft in anderer Form zu gestalten. Er findet deshalb als Ausblick Eingang in diese Arbeit.

Doch was genau verbirgt sich hinter diesem Begriff - "Digital Rights Management"?

1.2 Begriffsdefinition “Digital Rights Management”

Mark Stamp, langjähriger Entwickler von DRM-Software und mittlerweile in diesem Bereich als Assistant Professor des Department of Computer Science der San Jose State University tätig [23], definiert den Kerngedanken dieses Technologie-Konglomerates wie folgt:

Digital rights management (DRM) can be viewed as an attempt to provide ‘remote control’ of digital content. The required level of protection goes beyond simply delivering the digital content - restrictions on the use of the content must be maintained after it has been delivered. In other words, DRM requires ‘persistent protection’, i.e., protection that stays with the content. [24]

Dieser Gedankengang, der Sicherheit zum Prinzip erhebt, bildet die Grundlage aller DRM-Anwendungen und den eigentlichen Gegenstand dieser Arbeit. Systeme, die sich *ausschließlich* auf dieser Ebene bewegen, klassifiziert Renato Iannella [25] als der *Ersten Generation* des DRM zugehörig. Denn auf diese Schicht aufbauend definiert er weiter reichende Funktionalitäten, welche das System zur omnipräsenten Zentrale im Umgang mit allen Arten von Medien machen sollen – die *Zweiten Generation*:

Digital Rights Management (DRM) involves the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets – both in physical and digital form – including management of Rights Holders relationships. [26]

Beide Definitionen scheinen in der wissenschaftlichen Gemeinde Anerkennung gefunden zu haben, werden sie doch auch in anderen Arbeiten erwähnt (siehe z.B. [27]).

Zusammenfassend lässt sich also festhalten, dass es sich bei DRM um den Oberbegriff für eine Sammlung unterschiedlicher Technologien handelt. Diese können einzeln und für sich genommen durchaus noch in ganz anderen Bereichen Relevanz besitzen und mögen eventuell sogar zu ganz anderen Zwecken entwickelt worden sein. Im Bereich des DRM arbeiten sie jedoch zusammen, um die auf digitale Inhalte anwendbaren Rechte mit hinreichender Sicherheit durchzusetzen und darüber hinaus auch den gesamten Life-Cycle von Medien zu begleiten und zu gestalten. Was in diesem Zusammenhang “hinreichend” bedeutet, soll im Verlauf dieser Arbeit geklärt werden.

Eine weitere Begriffsabgrenzung sei hier noch kurz eingebracht: *Inhalt* (content) – die anglizistischen Fachbegriffe mögen eine Hilfe beim Studium der meist englischsprachigen Fachliteratur sein – im Zusammenhang mit DRM spielt immer auf sämtliche Ausprägungsformen *Geistigen Eigentums* (Intellectual Property, IP) in digitaler Form an. Das Spektrum erstreckt sich also von Stand- über Bewegtbilder und Klänge (Musik) bis hin zu digitalen Büchern und Artikeln, um nur eine Auswahl zu präsentieren. Streng genommen gehören auch Software-Systeme (als implementierte Algorithmen) zu diesem Feld, doch bedürfen die hier vorgestellten Techniken und Schemata einiger Anpassung, um auch auf dieses Feld applikabel zu sein.

2 Ein Blick über den Tellerrand

2.1 Von wirtschaftlicher Notwendigkeit...

Um die Entwicklung des Digital Rights Management in den letzten Jahren – angefangen mit ersten theoretischen Überlegungen hin zur mittlerweile zweiten Generation an Implementierungen – nachvollziehen zu können, scheint ein Exkurs in die Entwicklung der Wirtschaft im letzten Jahrhundert angebracht (die folgenden Ausführungen finden größtenteils in [20] ihren Ursprung):

Die sowohl nach neoklassischer wie auch nach liberaler Wirtschaftstheorie ursprünglichen Produktionsfaktoren Arbeit, Kapital und Boden wurden ab mitten des 20. Jahrhunderts zunehmend um den Faktor Wissen als zusätzlicher Nährboden der Wertschöpfung ergänzt. Aufbauend auf Rappaport's Theorie des *Shareholder Value*, die diesen nichtstofflichen Gütern (*Intangible Assets*) einen betriebswirtschaftlich hoch einzuordnenden, jedoch nicht bezifferbaren Wert zuordnete, wurde dem Wissen in seinen vielen Repräsentationen – der Übergang zu dem oben definierten Begriff *Inhalt* findet hier seinen Ursprung – eine Rohstoffartige Bedeutung zugeschrieben: Als Triebkraft der Wirtschaft und Entscheidungsfaktor für den Erfolg müssten Inhalte in ihrer Behandlung materiellen Rohstoffen gleich gestellt werden, sprich:

- Eigentum daran muss proklamiert werden können und
- Künstliche Verknappung zum Zwecke der Wertsteigerung soll ermöglicht werden

Natürlich gab es diese Tendenzen schon zuvor, und ihre ersten Ausdrucksformen liegen in den Anfängen des Patent- und Urheber-Rechtes begründet. Die allgemeine Sensibilisierung für die Thematik setzte jedoch erst mit den oben genannten Schritten ein, wie z.B. auch die auffallend häufigen Novellierungen des US-Amerikanischen Patentrechts seit jener Zeit, welche sich durch stetiges Anheben der Lebensdauer der Patente auszeichneten, zeigt.

Heutzutage sehen wir uns einer weit fortgeschrittenen Tertiärisierung der Wirtschaft gegenüber, und viele multinationale Großkonzerne wie beispielsweise Bertelsmann oder AOL Timer Warner handeln fast ausschließlich durch und mit Geistigem Eigentum. Und nicht nur diese Großen klagen darüber, dass ihnen ihre Felle – nicht davonschwimmen, sondern: – gestohlen werden [31]: Der Fall "Napster" und die damit assoziierten Erinnerungen sind wahrscheinlich vielen noch bewusst, und auch in der Literatur wurde er einschlägig diskutiert (z.B. [28], [29]). Man braucht eigentlich nur den Namen "Napster" als Platzhalter für z.B. "eMule" oder "KaZaA" anzusehen, um an dessen Aktualität erinnert zu werden.

Was ist geschehen? Wie konnte sich der Hoffnungsträger Wissen der 1950er Jahre zum Sorgenkind des neuen Jahrtausends mausern? Die Erklärung liegt in der Art der durch den Aufschwung der Datendienste und Digitaltechnik der 1990er Jahre geschaffenen neuartigen Verhältnissen: Geistiges Eigentum auf analogen physischen Trägern (z.B. als Buch, Schallplatte) bringt einen gewissen, dem Material innewohnenden Schutz mit sich, da hier immer noch echte, wenn auch im Vergleich zum eigentlichen Inhalt geringe

Werte involviert sind, welche es unter Aufwendung von Ressourcen zu replizieren gilt. Inhalte in digitaler Form jedoch, wie sie uns beispielsweise auf DVD oder im MP3- oder eBook-Format präsentiert werden, haben zwei grundlegend neue Eigenschaften:

- Die Möglichkeit zur verlustfreien Vervielfältigung ohne direkte Kosten aufgrund der digitalen Speicherung
- Die Möglichkeit der direkten globalen Verteilung ohne Zeitverlust über das Internet

Das Kapital vieler Firmen steht auf diese Weise – bildlich gesprochen – nackt am Pranger des globalen Marktplatzes, als Folge einer Wirtschaftspolitik, die vom technischen Fortschritt überrollt wurde. DRM tritt nun an, es dort wieder herabzuholen und – hübsch eingekleidet – in einem Schaukasten aus Panzerglas dem potentiellen Kunden darzubieten. Die neuen Märkte des Internet wollen erschlossen, und die Möglichkeiten digitaler Speicherung genutzt werden, es fehlt nur noch an der richtigen Berufskleidung für den Hauptakteur – sagt die Inhalte-Industrie...

2.2 Über differierende politische Ansichten...

Die Fakten – namentlich die grobe Anzahl illegalen Inhalte-Konsums – sind bekannt. Differenzen über deren Interpretation (ob beispielsweise jeder unrechtmäßige Download aus dem Netz eine Umsatzeinbuße im Sinne eines verlorenen Kunden darstelle?) sind jedoch üblich, und noch viel differenzierter sind die Meinungen zum Thema DRM allgemein:

So ist allein schon die Grundlage, ob nämlich Geistige Werte überhaupt als Eigentum im Sinne des entsprechenden Begriffs für physische Gegenstände zu verstehen seien, und ob die daraus abgeleiteten Rechte auf Besitz und Verknappung derselben hier überhaupt Anwendung finden dürften, umstritten. Federführend in dieser Debatte ist unter Anderen der Vordenker der Free Software Foundation, Richard Stallman [35], der in [36] dieses und andere "Missverständnisse" aufzuklären versucht. Und so völlig abwegig, wie es zuerst klingen mag, scheint dieses Ansinnen gar nicht zu sein: Was zum Beispiel die Möglichkeiten der Vervielfältigung, des Teilens, angeht, unterscheiden sich stoffliche und rein geistige Werte signifikant bezüglich des dabei auftretenden bzw. eben nicht auftretenden Werteverlustes. Und auch, dass man reale Produkte im Allgemeinen durch die Bezahlung vollständig erwirbt und danach mit ihnen nach eigenem Gusto verfahren kann, während man für Inhalte meistens nur eine bezüglich der Konsumentenrechte sehr restriktive Benutzungslizenz, jedoch kein Eigentum an der Sache, erhält, ist eine Tatsache. Man denke dabei nur an die EULA's ("End User Licence Agreement"), die jede moderne Softwareinstallation begleiten. Es sollte zumindest darüber nachgedacht werden, ob sich diese Ungleichheiten der zwei Arten von Eigentum nicht eventuell auch in unterschiedlicher Behandlung niederschlagen sollten.

Und auch abseits alter Hacker-Traditionen, die getreu dem Motto "my computer is my castle" die Kontrolle über jedes Bit der Maschine in der Hand des Benutzers sehen wollen und gemäß dem alten Kampfruf der 1980er Jahre Informationsfreiheit fordern [37], regen sich Stimmen, die für freien Informationsfluss zumindest in bestimmtem

Rahmen sprechen:

Die US-Amerikanische Juristin und Expertin für Patentrecht, Jessica Litman, beispielsweise sieht in der sogenannten "Globalen Allmende", dem der Weltöffentlichkeit frei zugänglichen Teil des Wissens oder *Public Domain* (PD), den alleinigen Ursprung für Innovation und damit Urhebertum, da Schöpfung heutzutage immer ein Akt der Rekombination vorhandener Strukturen anhand eigener Ideen sei [20]. Eine übermäßige Verknappung dieses Reservoirs würde ihrer Ansicht nach die Entwicklung einer Informationsgesellschaft eher aufhalten denn fördern, da diese somit ihrer Grundlagen beraubt würde. Nicht umsonst weist Richard Sietmann, Autor des betreffenden Artikels, auf die fein austarierte Gewichtung zwischen PD auf der einen und privatem Vermarktungsinteresse auf der anderen Seite hin, welches leicht aus der Waage zu fallen droht.

Mit der Informationsgesellschaft wird sich auch der "World Summit On The Information Society", ein von der UN-Organisation für Wissenschaft, Bildung und Kultur, UNESCO, geplanter internationaler Kongress, an welchem im Dezember 2003 viele Staats- und Regierungschefs teilnehmen werden, befassen [10]: In der zu unterzeichnenden Abschlusserklärung soll der freie und gleichberechtigte Zugang zu Informationen als politischer Wille festgeschrieben werden, zumindest, wenn man den ersten Entwurf einer Charta zugrunde legt. Auf dem Weg zur Wissensgesellschaft gäbe es mehr zu bedenken als die Geschäftsmodelle der Informationswirtschaft, meint denn auch die beteiligte Politikwissenschaftlerin Jeanette Hofmann.

Und der für die amerikanische Clintonregierung als Berater für eBusiness und Internet tätig gewesene Brian Kahin schließlich schreibt [14], dass es vielleicht besser wäre, Wertschöpfung im Zeitalter der wirtschaftlichen Tertiärisierung eher von besserem Service denn von stärkerem Schutz Geistigen Eigentums zu erwarten.

Auch gegen die Technik des DRM an sich werden Einwände vorgebracht: Zwar wird nicht überall so weit gegangen wie auf dem "Wissen ist was wert"-Kongress der Gewerkschaft ver.di [11] und von Orwell'schen Ausmaßen gesprochen, doch die Überwachung, die mit DRM Einzug in das heimische System halten könnte und sich gleichzeitig der Kontrolle seitens der Benutzer entzöge, verbreitet generell etwas Sorge. Die Angst der großen Masse an Verbrauchern vor einer ungewissen, aber auf jeden Fall – von deren Standpunkt aus gesehen – schlechteren, da unbequemeren und teureren Zukunft, braucht keine differenzierten Argumente, um sich Raum zu verschaffen, sie wird einfach ausgedrückt – und sollte abwägende Beachtung finden.

Die Großkonzerne hingegen rufen die Politik zu Hilfe [34], um möglichst schnell Rechtssicherheit zu erlangen, als Basis für nächsten Schritte. Und ihr Wunsch scheint erhört zu werden: Rund um den Globus beschäftigen sich Legislativen mit neuen Gesetzesentwürfen (eine Stellungnahme der Bundesregierung zum Thema findet sich unter anderem in [31]), die vornehmlich und entgegen der oben geschilderten Meinungen davon ausgehen, dass erweiterte Schutzmöglichkeiten für Inhalte einen Anreiz zum Erstellen neuer Werke böten und folglich rasch umzusetzen seien.

Im Folgenden sollen diese für den gesamten Themenkomplex maßgeblichen internationalen und nationalen Normen und Richtlinien nachgezeichnet werden:

2.3 Durch die Kraft des Gesetzes...

Aus rechtlicher Sicht ist die Frage nach DRM-Systemen gleichzusetzen mit der Frage nach dem Urheberrecht, da hier sowohl den Möglichkeiten und Rechten als auch den Schranken und Pflichten der Verbraucher wie auch der Anbieter Geistigen Eigentums eine wohldefinierte Form gegeben wird.

Doch da sich der Einfluss des Internets auf Inhalte um den gesamten Globus erstreckt, müssen auch entsprechende nationale Gesetze und Richtlinien eine möglichst weit reichende Verbreitung und vor allem Kohärenz aufweisen, um wirksam mit dieser Entwicklung Schritt halten zu können. Wie beispielsweise Sietmann und Kahin ([20], [14]) ausarbeiten, rief dieser Sachverhalt die Welthandelsorganisation WTO auf den Plan, deren Mitglieder 1994 das Abkommen zu den "Trade-Related Aspects of Intellectual Property Systems", TRIPS, verabschiedeten. 1996 wurde mit dem WIPO-Urheberrechtsabkommen der "World Intellectual Property Organisation" ein weiterer Schritt in Richtung Harmonisierung und Stärkung der Urheberrechte gemacht, eine Entwicklung, welche in den USA mittlerweile durch den "Digital Millennium Copyright Act" (DMCA) in nationales Recht umgesetzt ist. In der EU führte sie zu der "Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Rechte in der Informationsgesellschaft" (*Urheberrechtsnovelle*), welche in den Mitgliedsstaaten entweder schon umgesetzt ist (Stichtag war der 22.12.2002) oder momentan in den letzten Zügen der Bearbeitung liegt. In der Bundesrepublik beispielsweise wurde der Entwurf [30] in der Vorwoche des Osterfestes 2003 verabschiedet [3].

Es regen sich zwar Stimmen, die in den neuen internationalen Verträgen die Legalisierung eigentlich von der WTO geächteter Wettbewerbshindernisse sehen (die schon erwähnte Jessica Litman beispielsweise, nachzulesen bei Sietmann [20]), und gerade die Entwicklungs- oder Schwellenländer fürchten weitreichende negative Konsequenzen für ihre Volkswirtschaften, doch die etwa 160 Unterzeichner des TRIPS-Abkommens werden sich wohl als die stärkeren in diesem Konflikt erweisen...

Kernpunkt sowohl des DMCA als auch der europäischen Urheberrechtsnovelle ist der neue Status der Unantastbarkeit von Kopierschutz-Mechanismen: Dieses juristische Novum (im Folgenden wird auf die im deutschen Recht relevanten Paragraphen des Urheberrechts-Gesetzes, UrhG, noch genauer eingegangen) führt zu einer empfindlichen Störung des ehemals fein austarierten Verhältnisses zwischen Rechten und Pflichten im Urheberrecht:

Bis heute läuft das Vergütungssystem zwischen Urhebern und Konsumenten zweigleisig [22]: Für Bücher oder CD's beispielsweise bezahlt man im Handel den üblichen Betrag. Um die Gewohnheiten der Benutzer, die Inhalte untereinander gerne auch mal weitergeben, abzubilden, existiert zusätzlich eine Pauschalabgabe auf Geräte und Medien, welche zur Kopienerstellung geeignet sind. Diese ist bei deren Anschaffung (z.B.

CD-Rohlinge) oder Benutzung (z.B. Rundfunk) zu entrichten und wird über sogenannte Verwertungsgesellschaften wie die "GEMA" oder "VG Wort-Bild" nach internen Schlüsseln an die Urheber verteilt (Abbildung 1 illustriert das System). Dieses Recht auf *Privatkopie* (im amerikanischen Sprachgebrauch "*fair use*" genannt) ist in den Paragraphen 52a (Bereich Forschung und Lehre) und 53 (privater Bereich) des Urheberrechts-Gesetzes verankert und gilt auch weiterhin. Des weiteren muss der Inhalte-Anbieter wie bisher die Möglichkeiten zur Inanspruchnahme dieses Rechtes bereitstellen (§95b UrhG). Doch Paragraph 95a gewährt ihm nun das Recht auf Kopierschutz (welches keinesfalls unumstritten ist, manche Verbraucher reden bei einer kopiergeschützten CD beispielsweise von einem, das Recht auf Wandlung des Kaufvertrages einräumenden, Sachmangel, §462 BGB), und Paragraph 108b UrhG stellt dessen Umgehung zu gewerblichem Zwecke unter Strafe.

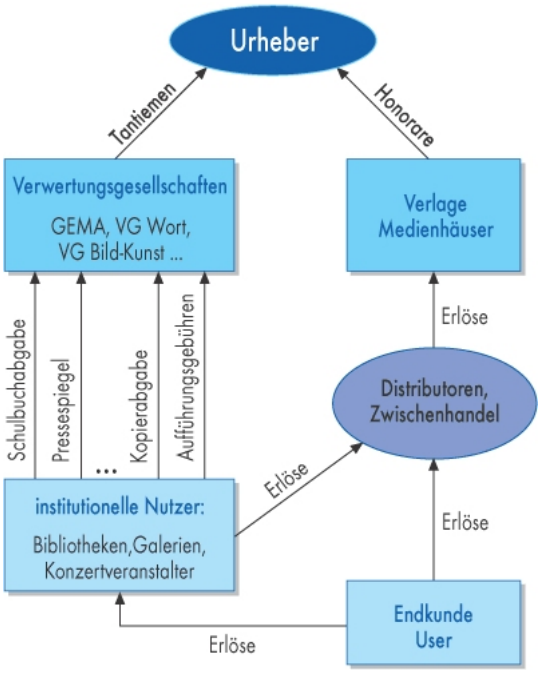

Abbildung 1: Das duale System der Urhebervergütung in Deutschland. Quelle: [20]

Doch nicht nur die Raubkopierer, Cracker und "Warez"-Anbieter können so gerichtlich belangt werden, für die Umgehung von "wirksamen technische Maßnahmen zum Schutz eines [...] Werkes" (so der Gesetzestext [30] zum Thema "Kopierschutz") stehen dem Rechteinhaber im privaten Bereich zivilrechtliche Mittel der Ahndung wie z.B. Schadensersatzansprüche offen.

Das Recht auf Privatkopie (in seiner althergebrachten Form) sei somit juristisch wenn schon nicht klar, dann doch zumindest eindeutig abgeschafft, schreibt denn auch Joerg Heidrich, Justiziar des Heise Zeitschriften Verlages [2]. Und die mit dem neuen Gesetz einhergehenden Änderungen in der Rechtsprechung tun somit Möglichkeiten auf, die zumindest in der Satire schon reichlich abstrakte (oder besser: abstruse?) Formen angenommen haben [38].

Wie dieses offensichtliche Dilemma gelöst werden soll, ist unklar: Die Politik hat entschieden, belässt allerdings wichtige Teile des Gesetzes, namentlich das öffentliche Zugänglichmachen geschützter Werke für Belange der Forschung und Lehre (§52a UrhG), in einer Art undefiniertem Schwebezustand: Es solle sich erst zeigen, ob die gefundenen Ansätze praxistauglich seien. Auch die Jusristen halten das Problem – zumindest für den Moment – für gelöst (nachzulesen in dem in [31] komplett enthaltenen Essay von Mathias Leistner), und von der Wirtschaft wird bestimmt kein Vorschlag kommen, sieht sie sich ihrem Wunsch von individualvergüteten Inhalten doch nun zum Greifen nahe.

Doch steuern die Bestrebungen verschärfter Rechtsmittel, die sich nicht nur in der Diskussion um DRM und das Urheberrecht, sonder auch auf den "Nebenschauplätzen" Softwarepatente und Restriktive Softwarelizenzen per Mausklick (in den USA durch den "Uniform Computer Information Transactions Act", UCITA, bereits geltendes Recht) finden, unsere Gesellschaft tatsächlich in die richtige Richtung, in eine ausgeglichenere Zukunft?

2.4 Zu einer Veränderung der Gesellschaft?

Wie Howard Rheingold in [15] am Beispiel des Mobilfunks erläutert, haben neue Schlüsseltechnologien immer auch einen prägenden Einfluss auf ihre Umwelt, die Gesellschaft. Und so, wie sich uns DRM heute präsentiert, wird es entweder eine Schlüsselrolle im Umgang mit sämtlichen Medien spielen oder ganz von der Bildfläche verschwinden (was wegen der dahinterstehenden Marktmacht der es vorantreibenden Medienkonzerne im Moment unwahrscheinlich erscheint). Diesen prägenden Einfluss gilt es auch und gerade als Entwickler abzuschätzen, es gilt, seine Verantwortung für die Menschen wahrzunehmen, welche die von einem entwickelten Technologien dann lange Zeit einzusetzen haben. Die Folgen des eigenen Handelns – in diesem Fall als Entwickler oder Entscheider von DRM- Systemen – sollten bewusst sein, und auch bereits vollzogene Schritte müssten sich kritischer Prüfung und gegebenenfalls Revidierung stellen, befindet denn auch das für Standardisierung im Internet zuständige W3-Consortium in seinem Workshop zum Thema DRM [32].

Grundsätzlich müssen zwei Ebenen der Einflussname durch DRM unterschieden werden, die zwar immer gekoppelt auftreten werden, deren Wirkungsbereiche jedoch disjunkt sind:

Der Bereich des Handels mit (Unterhaltungs-) Medien, der zwischen Konsument und Urheber bzw. Verwerter stattfindet, ist nur einer der beiden, wenn auch derjenige, welcher die aktuelle technische Entwicklung forciert und die Diskussionsforen füllt. Und hier werden sich, da DRM weniger ein Konstrukt zum Entwickeln neuer Vermarktungsstrategien für neue Märkte denn eines zum Anpassen neuer Märkte an bestehende, in anderer Umgebung gut funktionierende Verkaufspraktiken darstellt, eher die Konsumgewohnheiten der Käuferschaft verändern müssen: Es ist (zumindest bei den aktuellen technischen Ansätzen in Sachen DRM) fraglich, ob heutige Selbstverständlichkeiten wie das Hören eines erworbenen Musikstücks auf verschiedenen Abspielgeräten wie beispielsweise Stereoanlage und PC oder das weitergeben eines gekauften Videos an einen Freund (Dinge,

die laut UrhG unter den “fair use” fallen und somit legal sind), weiterhin möglich sein werden. Doch die Chancen für die Medienkonzerne stehen gut, glaubt man den Marktstudien, wie sie beispielsweise [33] zusammenfasst, und sowieso hätte das unorganisierte, nicht gerichtete Aufbegehren einer trägen Konsumentenmasse der Wirtschaftskraft geballter Lobbyarbeit der Industrie wenig entgegenzusetzen, wie Kahin in [14] am Beispiel der Umfragen zum Thema Softwarepatente verdeutlicht.

Der andere Bereich der Einflussnahme durch DRM tangiert diejenige Art von Information, die heute immer wichtiger wird: Nachrichten, Know-How, Wissen im Prinzip, auf welches man Entscheidungen gründen kann, oder umgekehrt: Wissen, ohne welches man keine Entscheidungen treffen kann, ohne das man hilflos ist. Es fließt normalerweise zwischen Firmen, aber auch zwischen Staaten oder aber auch zwischen dem Staat und seinen Bürgern. Und auch dieses Wissen wäre durch DRM total kontrollierbar, prinzipiell könnte also gezielt bestimmten Individuen (oder Gruppen, Schichten, Völkern, ...) Information vorenthalten werden. Andersherum wäre es möglich, den Abruf von Inhalten zu protokollieren, was datenschutzrechtlich höchst bedenklich, jedoch faktisch nicht nachweisbar wäre.

Solche Gedankenexperimente münden leicht in Orwell’sche Visionen, und die Grenze zwischen begründeter Vorsicht und Paranoia ist hier fließend. Das liegt zum Teil daran, dass die momentanen Technologieführer im Bereich des DRM, wie beispielsweise Intertrust, IBM, Microsoft oder RealNetworks, solchen Gedanken durch ihre Werbeaussagen von absoluter Kontrolle und Sicherheit der mit ihren Systemen geschützten Inhalte fördern. Doch was ist hier Fiktion der Marketingabteilung, was Realität der Technik? – Werfen wir einen “Blick unter die Haube”...

3 Die Technik hinter DRM

Für alle Betroffenen im Bereich DRM ist es essentiell, dass Klarheit über die Funktionsweise des Systems herrscht. Und dies gilt insbesondere für die sicherheitsrelevanten Funktionen, denn nur so können (potentielle) Kunden die zu erwartenden Veränderungen abschätzen, und Rechteinhaber die Dauerhaftigkeit des Schutzes evaluieren, dem sie ihre Werke anvertrauen.

Deshalb soll im Folgenden der Aufbau von DRM-Systemen in allgemeiner, schematischer Form skizziert werden, um anhand dessen deren Funktionsweise sowie die darunter liegenden Prinzipien genauer zu erläutern, wobei sich die Betrachtung auf die Bereiche, die zum Erlangen hoher Sicherheit zumindest peripher beitragen, beschränkt. Die Fakten, auf denen dieser Ansatz basiert, stammen zum größten Teil aus dem Artikel von Stamp [24], welcher als Einziger Hinweise auf den grundsätzlichen Aufbau dieses Teilbereiches von DRM-Systemen bietet. Die Synthese seiner Arbeit mit den Ergebnissen von z.B. [7], [22], [27] oder [32] floss in Abbildung 2 ein und legt den Grundstein für die hier gewählte Systematisierung:

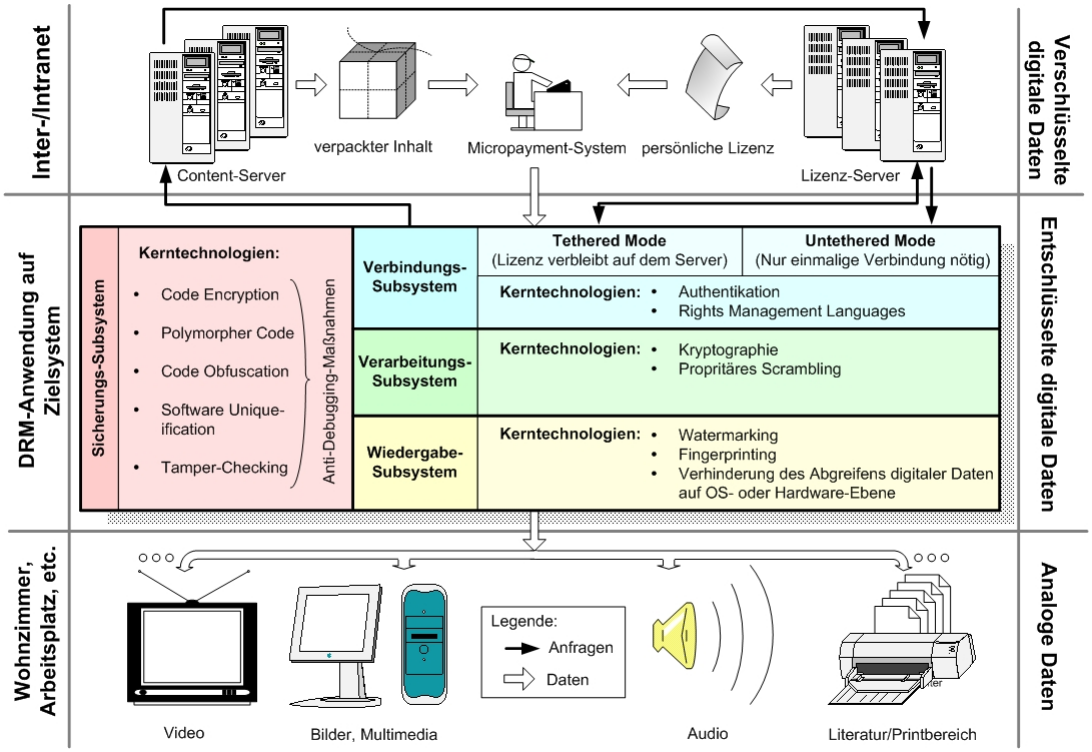

Abbildung 2: Ein allgemeines DRM-Schema, abgeleitet aus den verschiedensten Berichten zu Aufbau und Funktion von DRM-Systemen

Die Abbildung zeigt den Datenfluss der geschützten Inhalte von deren Aquisition aus öffentlichen Quellen bis zu ihrer Wiedergabe auf den Geräten des Endbenutzers, wobei auch der Vorgang des Anfragens der Daten skizziert ist. In der Mitte der Grafik ist der schematische Aufbau eines allgemeinen DRM-Systems zu sehen, bei welchem die in der oben genannten Literatur erwähnten Kerntechnologien so auf getrennte Subsy-

steme verteilt wurden, dass ein wohlbekanntes *"E-V-A"-Schema* entsteht: Eine *Verbindungsschicht* wickelt die Kommunikation mit den Servern der Inhalte-Anbieter ab, eine *Verarbeitungsschicht* erledigt die nötigen Transformationen, und eine *Wiedergabeschicht* schließlich sorgt für die Ausgabe in mediengerechter Form. Um die nötige Sicherheit für die mit großem Aufwand geschützten Inhalte auch auf dem Zielsystem des Anwenders zu gewährleisten, werden alle drei Schichten zusätzlich von der *Sicherungsschicht* umhüllt, die ein "knacken" des Systems verhindern soll.

Da es sich – in dem gegebenen Rahmen – um ein möglichst allgemeines Schema handelt, sind natürlich nicht alle Komponenten oder Abläufe in dieser Art in jedem realen System zu finden. So gibt es alleine zu dem Vorgang der Inhalte-Aquisition viele denkbare Variationen, und auch die Liste der verwendeten Techniken mag von dieser Auswahl abweichen. In der Realität der kommerziellen Produkte ist es sogar sehr wahrscheinlich, dass die Implementierung nicht sklavisch dem hier vorgeschlagenen Schichtenmodell folgt, sondern dem Arbeitsfluss entsprechend umgestaltet ist: "Watermarking" beispielsweise wird sicherlich schon vom Anbieter auf seine zum download bereiten Inhalte angewendet worden sein, und das Auslesen der Wasserzeichen könnte irgendwo im Programm passieren, es ist nicht an das Ende der Verarbeitungskette gebunden. Die gewählte Systematisierung scheint jedoch trotzdem sinnvoll, da sie, abseits syntaktischer Aspekte, die Semantik der Sicherheitskette von DRM-Systemen verdeutlicht und so einen schnellen Überblick über die prinzipielle Funktionsweise bietet.

Welche Aufgaben die einzelnen Subsysteme genau erfüllen, was sich hinter den von ihnen genutzten Kerntechnologien verbirgt, wie sie arbeiten und was sie leisten, und wie sich die Teile zu einem Ganzen subsummieren, wird im Folgenden – nach einer kurzen Betrachtung der Entwicklungsgeschichte des DRM sowie grundsätzlichen Überlegungen zur Realisierung – genauer betrachtet werden. Zuvor soll jedoch noch auf weiter von dem Sicherheitsprinzip abstrahierende Zusatzfunktionalitäten, wie Iannella sie in [26] schematisch darstellt, eingegangen werden:

3.1 Alternative Ansätze zur Schematisierung

Der Fokus dieser Arbeit liegt, wie bereits mehrfach anklang, klar auf dem Sicherheitsaspekt des DRM, was hauptsächlich auf dessen exponierte Stellung innerhalb der zum Ziel des DRM beitragenden Teilsysteme sowie den Mangel an speziell zu diesem Gebiet verfügbarer Literatur zurückzuführen ist. Doch als Potpourrie unterschiedlicher Teilbereiche hat DRM mehr zu bieten, als diesen zugegebenermaßen essentiellen Teil seiner selbst. Dieser Abschnitt widmet sich deshalb der kurzen Betrachtung weiter reichender Funktionalität, wie Iannella sie beschreibt, wissend, das darüber hinaus noch weitere Ansätze der Systematisierung existieren, welche in ihrer Gesamtheit wiederzugeben den Rahmen dieser Arbeit sprengen würde:

DRM-Systeme könnten von dieser Position aus betrachtet universelle Verwaltungswerkzeuge für den Umgang mit Inhalten und Rechten werden, also Werkzeuge, welche nicht nur digitale Rechte verwalten, sondern denen das Management *sämtlicher* Rechte

auf digitalem Weg obläge. Hierzu definiert Iannella zwei Schichten, welche diese High-Level-Methodik umsetzen:

- Die *Funktionale Architektur*: Hier wird eine Ende-zu-Ende-Verwaltung der Rechte über den gesamten Life-Cycle des Mediums auf hoher Abstraktionsebene definiert. Funktionen, welche die Erstellung (Definition) von Inhalt und Rechten ermöglichen, dessen anschließende Verteilung, und schließlich die Überwachung und Durchsetzung der Beschränkungen bei der Wiedergabe, sind Teil dieser Schicht. Der Schutzgedanke wird also verallgemeinert und in seinem Wirkungsgebiet ausgedehnt.
- Die *Informations-Architektur*: Ziel dieser Schicht ist es, die beteiligten Entitäten (Benutzer, Inhalt, Rechte) so zu modellieren, dass Beziehungen zwischen diesen ausgedrückt und verarbeitet werden können. Teil dieser Schicht ist beispielsweise eine Sprache zur Formulierung von Rechten, wie sie weiter unten noch Erwähnung finden wird.

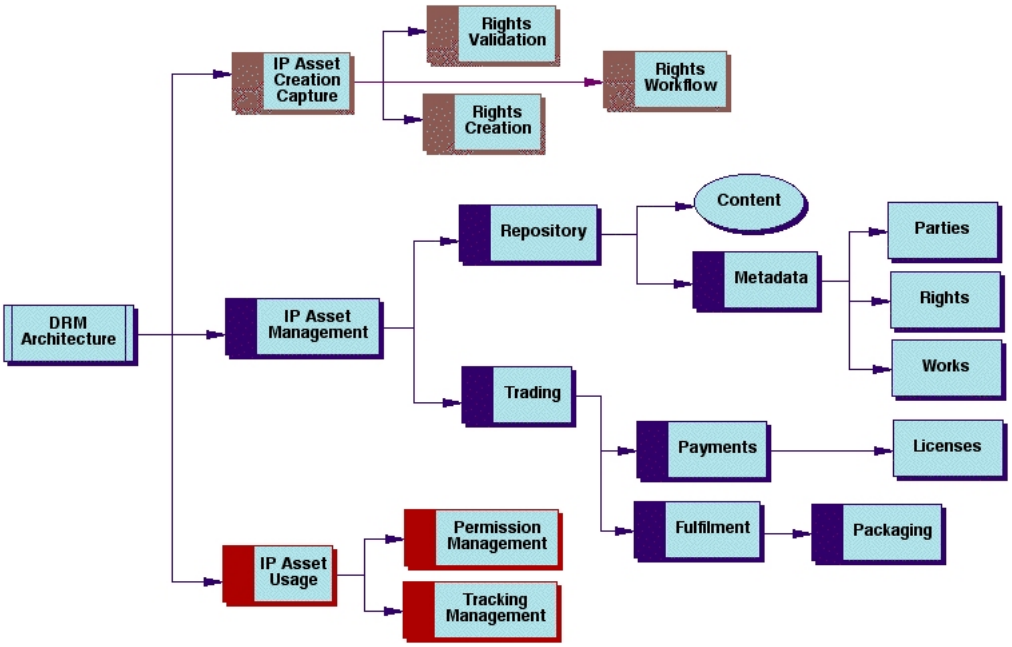

Abbildung 3: Schema der Funktionalen Architektur eines DRM-Systems nach Iannella. Quelle: [26]

Um dieses Architektur, wie Abbildung 3 sie illustriert, in der angestrebten Breite einführen zu können, wird ganz zu Recht die Frage nach allgemeingültigen Standards gestellt. Im Folgenden wird an geeigneter Stelle immer wieder darauf eingegangen werden, wobei nicht wenige der aufgeführten Standardisierungsbemühungen die Handschrift eben dieses Renato Iannellas tragen. Doch zurück zu den Aspekten der Systemsicherheit:

3.2 Vom "Honor System" zu technisch-wissenschaftlichen Ansätzen

Die historische Entwicklung von DRM-Systemen, wie Stamp sie darlegt, wirft kein gutes Licht auf die Pioniere der Branche: "*Security by Obscurity*", Sicherheit durch Uninformation, entpuppt sich seiner Meinung nach als Rückgrat vieler Sicherheitssysteme, was er mit einer Vielzahl von Fällen belegt, in denen DRM-Firmen Sicherheitsversprechen machen, aber deren Grundlage nicht näher erläutern. Diese Praxis prangert er entschieden an, denn schließlich wurde in der Kryptographie, dem wissenschaftlich am besten erforschten Teilgebiet für Sicherheitsfragen, schon vor langem das sogenannte *Kerckhoff'sche Prinip* entdeckt: Die Sicherheit eines Systems darf nicht von der Geheimhaltung des Algorithmus abhängen, sondern allein von der Geheimhaltung des Schlüssels [39]. Gründe für dieses Verhalten der Branche nennt Stamp nicht, es kann jedoch spekuliert werden, dass für viele Firmen der anfänglichen "Goldgräber-Zeit" galt: Wer nichts zu verbergen hat, verbirgt dieses wohl besser...

Abgesehen von diesen Verschleierungstaktiken stellt Stamp noch weitere DRM-Ansätze verschiedener Unternehmen in Frage, die hier exemplarisch dargestellt seien:

- Respekt: Adobe beispielsweise empfiehlt den Entwicklern von PDF-Betrachtern, die an eBooks oder geschützte PDF-Dokumente gebundenen Nutzungsrichtlinien der Urheber aus Respekt vor deren Werk zu berücksichtigen und entsprechende Sperren einzubauen. Dieses "honor system" stellt quasi keine Sicherheit bereit, hängt es doch nur vom guten Willen der Entwickler ab.
- Große Worte: Eine Firma namens "secretSeal" verspricht in ihrer Presseerklärung bahnbrechende Innovationen, welche sich bei genauer Betrachtung als unbedeutend oder schon lange bekannt erweisen.
- Patent-Überfluss: InterTrust, einer der Großen am Markt, weist in seinen Produktbeschreibungen zwar noch extra auf die notwendige technische Transparenz als Grundlage für Sicherheit hin, verweist dann jedoch nur auf sein riesiges Patent-Portfolio als Vertrauensgrundlage. Dass unter den vielen Patenten kaum ein technisches zu finden ist, wird verschwiegen...

Aktuelle Entwicklungen scheinen jedoch diese Erkenntnisse zu berücksichtigen. Und so haben Skandale wie um den DVD-Schutz "Contend Scrambling System" (CSS) oder das oben erwähnte eBook-Format [13], welche beide innerhalb kürzester Zeit "geknackt" wurden, zu einer neuen Generation von Produkten geführt, die nicht nur mehr Sicherheit versprechen, sondern auch auf ein solides Fundament wissenschaftlicher Theorien zu deren Durchsetzung bauen. Doch was bedeutet in diesem Zusammenhang überhaupt "mehr Sicherheit", wenn das angepeilte Endgerät per se völlige Sicherheit ausschließt und es am Ende doch nur 0 oder 1, sicher oder entsichert, gibt?

3.3 Die Grundfrage: Hardware oder Software?

Der PC erfreut sich seit gut 20 Jahren steigender Beliebtheit in weiten Kreisen der Bevölkerung. Das ist unter anderem darauf zurückzuführen, dass er architekturbedingt

ein offenes und universelles Gerät ist: Komponenten verschiedenster Hersteller sind verwendbar, und der Benutzer sieht es als sein Privileg an, über alle Vorgänge (zumindest theoretisch) die Kontrolle haben zu können.

Das beißt sich mit dem Ziel völliger Sicherheit für digitale Inhalte, denn als des Multimedia- Genießers liebstes Spielzeug bleibt der PC nun einmal Hauptzielplattform für Inhalte und damit auch für DRM, auch wenn dieses sich nicht im Bereich des PC's erschöpft. Und ein rein Software-basiertes Sicherheitssystem, so ausgeklügelt es auch seien mag, bleibt prinzipiell immer angreifbar und überwindbar, wenn die zugrundeliegende Architektur solches nicht verhindert.

Mit dem Ziel, diese Lücke zu schließen, entwickelt die TCG (Trusted Computing Group, ehemals [1] TCPA, Trusted Computing Platform Alliance) Möglichkeiten, wie unter Verwendung sicherer Betriebssysteme, die mit vertrauenswürdiger Hardware verdongelt werden sollen, auch der Alleskönner PC zu einem vertrauenswürdigen Bindeglied in der Kette des eCommerce werden kann. Microsoft arbeitet derweilen unter dem Decknamen "Next-Generation Secure Computing Base for Windows" (NGSCB, ehemals "Palladium", nachzulesen etwa unter [9]) an eben solch einer Betriebssystemerweiterung, und Infineon beispielsweise baut an einem "Trusted Platform Module" (TPM) genannten Chip, der obige Verdongelung realisieren soll. Mit diesem, einer fest im Rechner integrierten SmartCard gar nicht einmal unähnlichen, Baustein soll der PC nach außen eindeutig identifizierbar sein und somit eine berechenbare Größe im Geschäftsbetrieb darstellen können. Am Rande bemerkt ist, was in diesem Zusammenhang "vertrauenswürdig" bedeuten oder konkret, wer wem trauen können soll, jedoch nur eine unter vielen offenen Fragen im Zusammenhang mit diesem Konzept.

Ein ähnliches Bild zeigt sich auch auf dem Nebenschauplatz der Kopierschutzmechanismen für Audio-CD's: Da diese Form von Datenträgern ob der weiten Verbreitung von CD-Brennern über keinen inhärenten Schutz mehr verfügt, wird auch hier seitens der Plattenindustrie vermehrt auf (dieses mal dem Medium selbst anhaftende) Hardwareschutzmechanismen gesetzt. Eine detaillierte Darstellung und Bewertung der involvierten Techniken und Verfahren findet sich z.B. in [5].

Den beiden beispielhaft aufgeführten Ansätzen zum Erreichen höherer Sicherheit durch Veränderung der Hardware ist gemeinsam, dass hier höchste Sicherheit auf Kosten von verbreiteten, bewährten und beliebten Konzepten geschaffen wird: Denn eine derartige Veränderung der Hardwarebasis bringt in diesen Fällen immer auch eine Einschränkung der Funktionalität mit sich: Die Abwärtskompatibilität, so etwas wie die "Heilige Kuh" der IT-Branche der letzten Jahre, leidet, und Nutzungsbedingungen ändern sich. So lassen sich beispielsweise Kopiergeschützte Audio-CD's nicht mehr mit jedem Abspielgerät wiedergeben.

Doch es bleibt: Maximale Sicherheit lässt sich prinzipiell nur durch Hardwareeinsatz erreichen, und hier gilt es (wie so oft im Dunstbereich des DRM), für und wieder besonnen gegeneinander abzuwägen.

Für die weiteren Betrachtungen innerhalb dieser Arbeit jedoch soll dieses Dilemma ausgeblendet bleiben: Zum einen, da, wie Marktprognosen andeuten [33], die Hardwaregeschützen Wiedergabegeräte (vor allem die PC's) noch eine Weile auf sich warten lassen werden. Zum anderen, da die im folgenden dargelegten Methoden und Konzepte so universell gehalten sind, dass vieles davon auch auf Hardware-gestützte DRM-Systeme zutrifft, auch wenn explizit nur von Software-Systemen die Rede ist.

3.4 Das Verbindungs-Subsystem: Vom Geschäftsmodell zum Programm

Das Verbindungs-Subsystem ist innerhalb der Verarbeitungskette für die Aquisition der Inhalte und alle damit verbundenen Vorgänge verantwortlich. Hierzu zählen vor allem die Kommunikation mit dem Inhalte-Anbieter, die Authentifizierung des Benutzers gegenüber dem Server und der Empfang des Produktes inklusive der gültigen Nutzungsbedingungen (Lizenz).

Aufgrund des Schnittstellencharakters dieser Schicht als Verbindung zwischen Anbietersystem und Zielsystem lassen sich zwei prinzipielle Aussagen über sie treffen:

Erstens, dass das System öffentlich breit diskutiert ist. Literatur zum Thema DRM nimmt, sofern es um die verwendeten Techniken geht, fast ausschließlich Bezug auf das Verbindungssubsystem. Dieses ist auch einleuchtend, denn hier tritt der Kunde mit dem Anbieter direkt in Kontakt, so dass ihm Bedienung und Funktionsweise bekannt sein müssen. Man möchte informiert sein darüber, welche persönlichen Daten ausgetauscht oder preisgegeben werden, ob Kosten entstehen, oder wann und zu welchem Zweck Verbindungen zu externen Netzen erfolgen (hierzu im Anschluss mehr). Im Gegensatz zum Thema Sicherheit der erworbenen Inhalte wollen die Nutzer Fakten sehen, wenn es um die Sicherheit ihrer persönlichen Daten (der Privatsphäre) geht, und das schlägt sich scheinbar auch in der Ausgestaltung der Literatur nieder.

Zweitens, dass das System stark abhängig vom Vertriebsmodell des Anbieters ist. Inhalte können in unterschiedlicher Form zu verschiedenen Zwecken von den vielen Anbietern, deren Motive differieren, bereitgestellt werden. Und für jeden dieser Fälle mag DRM interessant sein, sei es zum Schutz der eigenen Tantiemen im Bereich Verkauf von Musik und Video für den Endbenutzer oder zur Wahrung von Betriebsgeheimnissen innerhalb einer großen Firma. Und in jedem dieser Fälle wird sich das Verbindungssubsystem etwas anders verhalten müssen. So wird beispielsweise in letzterem Fall ein Bezahlsystem obsolet sein, in ersterem jedoch essentiell.

3.4.1 Tethered vs. Untethered

Prinzipiell gibt es, sobald die eigentlichen Inhaltsdaten vom Server angefordert, eventuell bezahlt und schließlich heruntergeladen wurden, zwei Möglichkeiten, wie die anzuwendende Rechte verwaltet werden sollen:

Im sogenannten “Tethered Mode” (im neudeutschen Sprachgebrauch etwa “Online-Modus”, “Verbundener Modus”) verbleiben alle Schlüssel, die zum Öffnen des Inhaltes notwendig sind, auf dem Lizenzserver. Der Benutzer muss immer, sobald er auf den Inhalt zugreifen will, den Server kontaktieren, und basierend auf seinen aktuellen Nutzungsdaten und der persönlichen Lizenz wird ihm dann der Zugriff gestattet. Für den Anbieter der Inhalte hat das viele sicherheitstechnische Vorteile, denn die sensitiven Daten verbleiben so nicht in der Obhut des potentiell feindlichen Kunden. Und obwohl für den Kunden aufgrund der immer nötigen Verbindungen zur zentralen Instanz des Anbieters unbequem, ist diese Betriebsart in aktuellen Systemen weit verbreitet.

Kundenfreundlicher, allgemeiner, aber auch unsicherer gestaltet sich der Betrieb von DRM im “Untethered Mode” (“Offline-Modus”, “Ungebundener Modus”). Die Schlüssel werden mit Inhalt und Lizenz bei der Aquisition auf dem Zielsystem gespeichert und verbleiben dort, weitere Kontaktaufnahmen zu öffentlichen Servern entfallen.

Doch dadurch ergibt sich ein weiteres Problem: An welche Entitäten sollen die Benutzungsdaten (beispielsweise die Zahl der Aufrufe, falls diese im Rahmen der Lizenz überwacht werden müssen) gebunden sein? Liegen sie bei der Hardware, lässt sich ein Musikstück beispielsweise nur noch auf dem PC hören, der Genuss über den CD-Player im Wohnzimmer oder das Autoradio wäre nicht erlaubt. Bei einer Bindung an den Inhalt selbst müssen nur die Daten im Originalzustand wiederhergestellt werden, um die Rechte erneut zu erhalten. Und bei Kopplung von Rechten an Benutzer kann ein weiterer (mit der ersten realen Person durchaus identischer) Benutzer dem System gegenüber angemeldet werden, der über dieselben Zugangsdaten (Schlüssel, Passwörter, etc.) verfügt und so wieder alle Rechte genießt. Es gilt also wieder, abzuwägen: In diesem Fall Benutzbarkeit, was für die Kundenbindung wichtig ist, gegen Sicherheit, um unrechtmäßigen Gebrauch zu verhindern.

3.4.2 Authentikation

Wie Diana Kelley in [40] anhand vieler Studien und Argumente belegt, ist die sichere Authentikation oder auch *Identifizierung* des Benutzer gegenüber dem System des Anbieters die entscheidende Grundlage für eBusiness. Dass es auch zur Grundlage des DRM beiträgt, lässt sich leicht veranschaulichen, wenn man den neben dem Verkauf digitaler Inhalte zweiten großen Anwendungsfall des Sicherns geheimer/wichtiger Informationen durch DRM betrachtet: Das System muss wissen, ob der eingeloggte Benutzer jener ist, für den er sich ausgibt, denn was bedeutet stärkste Sicherheit bei Versand und Behandlung der Daten, wenn sie in die falschen Hände geschickt wurden?

Es existieren mittlerweile multiple Techniken zur Gewährleistung einer den an sie gestellten Sicherheits-Ansprüchen gerecht werdenden Identifikation von Kommunikationspartner. Das Spektrum reicht dabei von den recht unsicheren Passwörtern [41] am unteren Ende der Skala bis hin zu auf moderner Kryptographie (siehe unten) beruhenden Public-Key-Infrastrukturen (PKI), welche von vertrauenswürdigen Instanzen gefertigte Digitale Zertifikate der Benutzer zu deren Erkennung einsetzen. Einen Überblick über verschiedene Merkmale, welche zur Authentikation eingesetzt werden, verschafft Abbil-

dung 4.

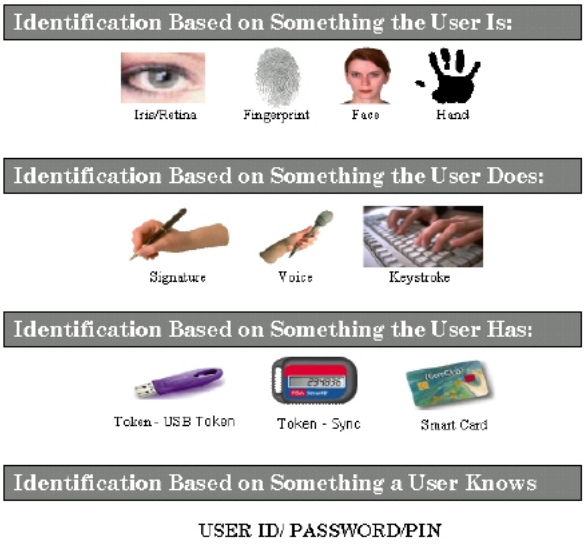

Abbildung 4: Möglichkeiten der Authentikation. Je nach dem, ob eine oder mehrere Arten gleichzeitig genutzt werden, unterscheidet man zwischen Single-Factor und Multi-Factor-Techniken. Quelle: [42]

Auf diesem mit den Belangen des eBusiness wachsenden Markt tummeln sich mittlerweile viele Anbieter von Komplettlösungen. Doch für den DRM-Bereich ist es vor allem wichtig, dass die potentiellen Benutzer nicht für jeden Dienst unterschiedlicher Anbieter andere Mechanismen anzuwenden brauchen: Wenn jemand Musik online kaufen möchte, will er dafür nicht mehrere Passwörter, Zertifikate oder SmartCards vorhalten müssen, sondern möglichst zentral verwaltet auf Shopping-Tour gehen. BioNetrix nennt das “Single Sign On” [42], und Microsoft versucht seit geraumer Zeit, mit seinem .NET-Passport-Dienst [43] genau in diesem Bereich Fuß zu fassen. Doch im Moment sind die Publikumsreaktionen ob schlechter Schlagzeilen die Privatsphäre der Kunden betreffend noch recht verhalten, um es gelinde auszudrücken [44].

Auf ein weiteres Problem im Zusammenhang mit der Verbindungsschicht und Authentikation sei hier noch kurz hingewiesen: Die in diesem Bereich verwendeten Schlüssel, Zertifikate, Passwörter etc. sind natürlich äußerst sensitive Daten und präferiertes Ziel für einen Angriff auf das System. Es müssen also leistungsfähige Mechanismen bereitgestellt werden, die ein effizientes und vor allem sicheres Schlüssel-Management und -Caching betreiben. Solche werden im Kapitel über das Sicherungs-Subsystem eingehender betrachtet.

3.4.3 Rights Management Languages

Dieser Abschnitt beschäftigt sich mit den Techniken zur formalen, also maschinenlesbaren Niederschrift von Rechten. Grundsätzlich lässt sich dieses Problem mit einer beliebigen *Markup-Sprache* abhandeln, doch es existieren besondere Anforderungen an diesen

Bereich, die ein spezialisierteres Werkzeug nötig machen. Hier sei deshalb auf die Standardisierungsbemühungen der ISO sowie der MPEG für eine solche *Rights Management Language* als Indikator für deren Relevanz das Thema betreffend hingewiesen [45].

Momentan existieren zwei Ansätze, diesem Begehren gerecht zu werden. Sie sind sich grundsätzlich sehr ähnlich, basieren sie doch beide auf der Beschreibungssprache XML als Grundgerüst, für die sie jeweils verschiedene XML-Schemata bzw. "Data-Dictionarys" definieren.

"Open Digital Rights Language" (ODRL) nennt sich der erste Ansatz, welcher in [46] spezifiziert wird. Ziel dieser Initiative ist es, einen offenen und erweiterbaren Standard für die Formulierung digitaler Rechte und Beschränkungen für das eBusiness vorzulegen [47]. Die Sprache soll zusätzlich schlank, universell und standardisiert sein.

Mit ähnlichen Zielen hat mittlerweile jedoch die Sprache XrML (eXtensible rights Markup Language) größere Bedeutung gewonnen. Entwickelt wurde sie vor einigen Jahren unter dem Namen DPRL (Digital Property Rights Language) am Palo Alto Research Center der Firma Xerox, doch zwischenzeitlich wurde sie (wohl wegen des steigenden Bekanntheitsgrades des ähnlich klingenden XML) umbenannt. Da sie wie bereits erwähnt mit ODRL vergleichbare Möglichkeiten mit breitem öffentlichen Anklang und guter Dokumentation verbinden kann, soll der Rest dieses Abschnittes XrML als Sprache für die Formulierung digitaler Rechte etwas genauer beleuchten, unter der Annahme, dass Ähnliches auch für ihre Konkurrentin gilt:

Das Grundgerüst einer jeden XrML-basierten Lizenz für digitale Inhalte ist die `<license>`. Sie besteht grundsätzlich aus einer oder mehreren `<grant>`-Zusicherungen, also Abschnitten, die jemandem etwas gewähren. Formal wird dieser Vorgang durch die folgenden vier Tag-Typen ausgestaltet, wie auch Abbildung 5 illustriert:

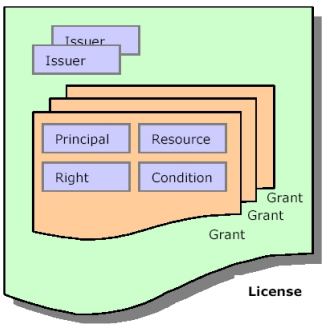

Abbildung 5: Der prinzipielle Aufbau einer Lizenz in XrML. Quelle: [48]

- `<principal>`: Die Entität, für welche die Lizenz gilt. Grundsätzlich ist ein Principal ein Individuum; Gruppen von Individuen lassen sich jedoch über das sprachliche Mittel der variablen Definition und der Mustererkennung implementieren.
- `<right>`: Das Recht, welches auf die...
- `<resource>`: Den digitalen Inhalt ... angewendet werden soll

- `<condition>`: Die Umstände, unter denen das Recht gilt (z.B. zeitliche Beschränkung)

Jeder dieser vier Typen wird im konkreten Fall einen von mehreren möglichen Werten annehmen. So kann der `<principal>` ein `<keyHolder>` sein oder die `<resource>` ein Stück `<digitalWork>`, und beides wird durch weitere Tags näher beschrieben und erläutert. Ein dem XrML-SDK [49] entnommenes Beispiel mag zur Verdeutlichung beitragen:

```
<license>
  <grant>
    <keyHolder>
      <info>
        <dsig:KeyValue>
          <dsig:RSAKeyValue>
            <dsig:Modulus>Fa7wo6NYf...</dsig:Modulus>
            <dsig:Exponent>AQABAA==</dsig:Exponent>
          </dsig:RSAKeyValue>
        </dsig:KeyValue>
      </info>
    </keyHolder>
    <cx:print/>
    <cx:digitalWork>
      <cx:locator>
        <nonSecureIndirect URI="http://www.xrml.org/reference"/>
      </cx:locator>
    </cx:digitalWork>
  </grant>
</license>
```

Hier wird einem bestimmten `<keyHolder>` das Recht `<print>`, anzuwenden auf `<digitalWork>` unter der URL `<locator>`, zuerkannt. Diese Lizenz könnte nun noch von ihrem Herausgeber, `<issuer>`, digital signiert werden, um ihre Echtheit zu bestätigen.

Für XrML existieren zusätzlich zwei nennenswerte Erweiterungen: Das ”Standard Extension Schema”, welches generell weit verbreitete Anwendungsfälle für die Sprache abdeckt, die es nicht in den schlanken Standard geschafft haben, sowie das “Content Extension Schema”, welches speziell für den DRM-Sektor wichtige Spezifikationen bereitstellt. Somit ist XrML gewappnet für nahezu jede Anforderung, die an die Formulierung von Rechten gebunden sein könnte.

3.5 Das Verarbeitungs-Subsystem: Umkleide für den Inhalt

Der oben empfohlenen Struktur folgend, hat die Verarbeitungsschicht die Aufgabe, die ankommenden beziehungsweise lokal vorhandenen Inhalte so aufzubereiten, das sie von

der Wiedergabeschicht ausgegeben werden können. Faktisch bedeutet das, die Verschlüsselung zu dechiffrieren, und die Nutzdaten von anderen Anweisungen wie beispielsweise der Lizenz zu trennen. Denn üblicherweise sind per DRM geschützte Inhalte zu einer Art "Container" verpackt, der entsprechend dem übergeordneten Ziel Inhalt und Nutzungsbedingungen aneinander bindet.

Diese Ver- und Entschlüsselungstechniken fallen in den Bereich der Kryptographie, eines Teilgebietes der Mathematik. Während sich dieses noch mit vielen weiteren Themen befasst, sollen im folgenden kurz die für den Bereich dieser Arbeit relevanten Verfahren erläutert werden:

3.5.1 Kryptographie

In den Anfängen des Digital Rights Management (und landläufig vielerorts noch heute) wurde dessen Aufgabe mit der eines Kopierschutzes gleichgesetzt. Folglich wurde Verschlüsselung (respektive deren Umkehrung) als Hauptaufgabe des Systems gesehen. Doch diese Agenda hat sich geändert, wie die eingangs zitierten Passagen aus den Aufsätzen Stamps und Iannellas zeigen. Doch auch, wenn sie nicht mehr als hinreichend betrachtet werden, wie beispielsweise auch der Anteil der Kryptographie am Gesamtumfang eines Dokuments für Sicherheitsfragen der EU-Kommission "Scientific and Technical Options Assessment" zeigt [50], notwendig bleiben kryptographische Techniken für diese Domäne allemal.

Verschlüsselung (respektive ihrer Umkehr) kann prinzipiell auf zwei unterschiedliche Arten erfolgen: Mittels *geheimer* Schlüssel (private Keys) oder unter Verwendung von *öffentlichen* Schlüsseln (public Keys).

Die erste Methode, auch *symmetrische* Verschlüsselung genannt, basiert dabei auf einem Schlüssel `k`, der nur den beiden Kommunikationspartnern bekannt sein darf. Der Absender parametrisiert die gemeinsame Verschlüsselungsfunktion `f` mit diesem Schlüssel und wendet sie dann auf den Inhalt `m` an, so dass die kodierte Form `c` entsteht: $c = f_k(m)$. Diese kann über einen potentiell unsicheren Kanal (beispielsweise das Internet) übertragen werden, ohne dass eine Penetration der Vertraulichkeit der Daten befürchtet werden muss. Der Empfänger enthält durch Umkehrung des Chiffrierungsalgorithmus wieder die Originalform des Inhalts zurück: $m = f_k^{-1}(c)$. Bekanntester und am weitesten verbreiteter Algorithmus dieser Art ist der AES, "Advanced Encryption Standard", welcher Aufgrund seiner kryptologischen und praktischen Sicherheit sowie seiner Geschwindigkeit auch in vielen DRM-Systemen Anwendung findet. AES löste vor kurzem den erwiesenermaßen unsicher gewordenen DES, "Data Encryption Standard", ab.

Allerdings stellt sich noch das Problem der Übermittlung der geheimen Schlüssel ohne die Anwesenheit eines sicheren Übertragungskanals. Für diesen Fall wird die *asymmetrische* Verschlüsselung mittels öffentlicher Schlüssel verwendet: Jeder Kommunikationsteilnehmer besitzt ein Schlüsselpaar `{e, d}`, dessen einer Teil `e` öffentlich bekannt ist, der andere jedoch nicht. Soll ein Teilnehmer `A` verschlüsselte Daten erhalten, werden die-

se mit *dessen* öffentlichem Schlüssel e_A verschlüsselt: $c = f_{e_A}(m)$. Entschlüsselt werden kann dieser Inhalt nun nur noch mit dem zugehörigen Schlüssel d_A des Empfängers `A` gemäß $m = f_{d_A}(c)$. Theoretisch untermauert wird dieses Phänomen durch ein Teilgebiet der Mathematik, die Zahlentheorie, sowie durch Sätze, die sich bis auf Euler und Fermat zurückführen lassen.

Der am häufigsten eingesetzte Algorithmus dieser Art nennt sich RSA, benannt nach seinen Entwicklern Rivest, Shamir und Adleman. Er besitzt wie seine Artgenossen den symmetrischen Verfahren gegenüber den Vorteil, dass kein Schlüsseltausch erfolgen muss und so die gesamt Kommunikation über unsichere Kanäle erfolgen darf. Doch wegen der um den Faktor 1000 höheren Laufzeit dieser Verfahren werden sie in der Verschlüsselung praktisch nur zum sicheren Versand der geheimen Sitzungs-Schlüssel für die Private-Key-Kryptographie verwendet.

Abseits dieser Domäne können sie jedoch, wie bereits weiter oben im Text anklang, als wichtige Bestandteile von Authentikationsmechanismen und der Lizenz-Bildung verwendet werden, da Public-Key-Systeme das Grundgerüst digitaler Signaturen und Zertifikate darstellen:

Ein Urheber `A` zertifiziert die Echtheit eines Dokumentes `m`, indem er an dieses eine mit seiner geheimen Signaturfunktion s_A erzeugte, für das Dokument eindeutige Prüfsumme `sig` anhängt: $sig = s_A(m)$. Der Empfänger kann nun mithilfe der öffentlichen Verifikationsfunktion v_A des Urhebers von `sig` auf `m` schließen und so dessen Urheberschaft sowie die Unversehrtheit des Inhalts bestätigen ($m = v_A(sig)$). Eine tiefere Erklärungen dieses und der anderen genannten Verfahren findet sich beispielsweise in [39], wo auch auf weitere Implementierungsdetails und Standardisierungs-Bemühungen eingegangen wird.

3.5.2 Propritäres Scrambling

Neben den gesicherten Erkenntnissen der Kryptographie wird in diesem um höchste Sicherheit bedachten Aufgabengebiet zusätzlich auf propritäre Scramble-Methoden (und entsprechende DeScramble-Methoden) zurückgegriffen. Dabei handelt es sich im weitesten Sinne um Funktionen, die den Inhalt reversibel unlesbar machen, also verschlüsseln, was als Ziel zuerst einmal identisch mit demjenigen der Kryptographie ist. Unterschiedlich ist jedoch, dass der Algorithmus hier öffentlich unbekannt ist und dieses auch bleiben muss. Doch zu welchem Zweck, wo doch hier keine theoretische Grundlage die Sicherheit belegt?

Natürlich gilt auch dort das oben bereits erwähnte Kerckhoff'sche Prinzip, doch geht es hier um die Handhabung von Informationen, und deren Wert hängt zumindest teilweise von der zeitlichen Komponente ab. Wenn das Vorhandensein eines unbekannten Verschlüsselungsprinzips einen potentiellen Hacker nur einige Zeit länger mit dem Vorgang des Reverse Engineerings aufhält, hat es seinen Zweck erfüllt.

Diese Erkenntnis leitet direkt über zu den Aufgaben und Funktionalitäten der Siche-

rungsschicht:

3.6 Das Sicherungs-Subsystem: Streben nach Unverwundbarkeit

Nun liegen die Inhalte zumindest so lange, wie sie vom Benutzer betrachtet werden, in entschlüsselter, digitaler Form auf dem Zielsystem des Anwenders vor. Es ist also an der Zeit, einige Worte über die Sicherheit des DRM-Systems als DV-System an sich zu verlieren, denn nur noch dieser Käfig trennt nun die Daten von der DRM-freien "Wildbahn".

Um was es also in der Sicherungs-Schicht geht, sind (ganz losgelöst von der Thematik DRM) Techniken, die ein "Debuggen" des Systems – d.h. ein extrahieren der zur Laufzeit im System vorhandenen Daten oder der zur Verarbeitung benötigten Algorithmen – wenn schon nicht zu verhindern, dann doch zumindest beliebig komplex werden zu lassen, so dass potentielle Angreifer abgeschreckt werden und die Zahl der Sicherheitsverletzungen gering bleibt. Weiterhin soll bis zu einem bestimmten Grad gesichert werden können, dass der Einbruch in eine spezielle Instanz nicht die Sicherheit des global vielfach installierten Systems kompromittiert.

Im Folgenden werden Techniken besprochen, die solches speziell für (PC-)Software-Systeme leisten. Doch wie schon in den vorangegangenen Kapiteln gilt auch hier eine gewisse Portabilität der Prinzipien auch auf anderen Architekturen. Generell dienen solche *Anti- Debugging-Maßnahmen* also dem Ziel, das Reverse Engineering des schützenswerten Objektes so kompliziert wie möglich zu machen und so ein Optimum (nicht das für Software unerreichbare Maximum) an Sicherheit zu schaffen.

Zuvor vielleicht noch eine kurze Erläuterung zu der Portabilität von Anti-Debugging-Techniken auf reine Hardware-Systeme, die so vielleicht nicht direkt einleuchtend erscheinen mag: Nach dem jetzigen Stand der Dinge sowohl in der Halbleitertechnik als auch in der Softwarearchitektur ist es nicht mehr möglich, eine eindeutige Grenze zu finden zwischen dem Ende der Hardwareschicht und dem Anfang von Software: Prozessoren werden mit μCode ausgestattet, und beim Entwurf einer digitalen Schaltung spricht man von der "Programmierung" des EPROMs oder allgemein des Logik-Gatters. Software andererseits vermag mittlerweile die Emulation ganzer PC-Architekturen, wie das Projekt VMware auf beeindruckende Weise verdeutlicht. Code steckt folglich in beidem, unterschiedlich ist allein dessen physikalische Repräsentation. Da dieses keinen prinzipiellen (höchstens einen qualitativen) Unterschied für die Anwendbarkeit von Reverse Engineering macht, sind folglich auch entsprechende Gegenmaßnahmen sowohl auf Hard- als auch auf Software anwendbar.

Wie solche noch vor einigen Jahren auf dem PC aussahen und was sie leisteten, zeigt beispielsweise [51] auf. Durch moderne Betriebssysteme, die den expliziten Zugriff auf Interrupttabellen und andere Systemressourcen verhindern, sind solche Debugger-Erkennungs-Routinen mittlerweile jedoch sehr stark plattformabhängig, und generelle Methodiken lassen sich schwer extrahieren. Es folgen daher Beispiele weniger System-

naher, universellerer Methoden, auch wenn die Wichtigkeit der Debug-Disruptoren für das Zusammenspiel aller Teilkomponenten unverändert hoch ist:

3.6.1 Code Encryption

Die Verschlüsselung des ausführbaren Programmcodes (und seiner Daten) erfolgt derart, dass zur Laufzeit des Systems immer nur kleinste Blöcke, welche wirklich gerade zur Verarbeitung anstehen, dechiffriert und ausgeführt werden. Sämtliche latente Teilbereiche verbleiben vor und nach ihrer Benutzung verschlüsselt im Speicher. Wählt man die Blockgrößen geschickt, lässt sich so ein Plus an Sicherheit mit akzeptablen Geschwindigkeitsbußen erzielen.

Interessanterweise findet sich Anleitung gebende Literatur zu diesem Thema fast ausschließlich im Bereich der Hacker- bzw. Virus-Szene, wie das illustre Pseudonym des Autors von [53], "NightmareJoker", verdeutlicht. Nichtsdestotrotz finden sich hier gute Codebeispiele (für die Sprache Visual Basic), welche die Arbeitsweise verdeutlichen.

3.6.2 Polymorpher Code

Auch in diesem Gebiet scheint einführende Literatur nur aus dubiosen Quellen [52] zu stammen. Doch erneut ist das Resultat sowohl legal als auch wirkungsvoll:

Es geht darum, ein Programm (oder Teile desselben) immer wieder unterschiedlich aussehen, aber identisch funktionieren zu lassen. Möglich wird das beispielsweise durch Code-Encryption, wie sie im vorangegangenen Abschnitt beschrieben wurde, mit sich ändernden Schlüsseln. Was bleibt, ist der Ver- /Entschlüsselungsteil, der gezwungenermaßen statisch bleibt. Nun existieren verschiedenen Ansätze, an dieser Stelle Dynamik in das System zu bringen:

- Mehrere Crypt-Komponenten, aus denen nur jeweils eine zum Einsatz kommt
- Mehrere Instruktionen für Teilbereich innerhalb dieser Decryptoren

Durch Kombination dieser Möglichkeiten und dem Bilden von Permutationen (d.h. in der Ausführungsreihenfolge vertauschten Code-Abschnitten) ergeben sich genug Möglichkeiten, die Ausführung des Programms dynamisch aussehen zu lassen und so das Erstellen von Suchmustern zu Angriffszwecken effektiv zu verhindern.

3.6.3 Code Obfuscation

Code (oder Programm-) Obfuscation befasst sich mit den Möglichkeiten, Quellcode so zu schreiben und zu strukturieren, dass ein uneingeweihter Betrachter nicht auf dessen Funktion schließen kann. Hierzu werden Transformationen am Code vorgenommen, welche die Syntax und Struktur verändern, die Semantik nach außen jedoch erhalten. Praktisch könnte das etwa wie folgt aussehen:

```
#!/usr/bin/perl
# Len - http://www.perlmonks.org/index.pl?node_id=176043

$_='
         $q ="\                    47"; wh
        ile                            ($ ;=
      $z                 +=               .5 ){
    %c=            $r=0;$/ ="";whi          le(2
   0+           $z>($;+=.05)){$c{int$       _+ 2
  6+          2*($               r+= .0       2) *
 s           in$                    ;}{1       -$_
+1          0+            int        $r*c       o s
$          ;}          =1for(0.       .1)        }$
t         =r          ever se;$        /.        =‘
c         le         ar     ‘.         "         #!
/         usr        /bi              n/         pe
rl        \n\        $_ =$q         \n"          ;
fo         r$y         (1..20){$c{$_}          {
$ y        }? $          /.=chop$t             :
 ($/         . ="                             \4
 0")          for(0.                        .53)          ;
   $/.         ="\n"}pri              nt"$/$          q;
   s; ".          chr(9 2)."s;;g;eval\n          "}
';s;\s;;g;eval
#$
```

Dieses Beispiel, durch einen Perl-Interpreter geschleust, erzeugt ein ASCII-Bild, welches dem Layout des Sourcecodes entspricht, was nach dessen Lektüre jedoch auch dem geübten Leser nicht sofort ins Auge springt. Es entstammt der Arbeit von Thomas Klausner anlässlich der Linuxwochen 2002 [54], die eher den künstlerischen Aspekt von Obfuscation-Techniken beleuchtet. Hintergrund dessen ist jedoch eine solide wissenschaftliche Theorie [55], deren Zweck der Schutz von Software vor Reverse Engineering ist.

Collberg und Thomborson, deren grundlegende Arbeiten über Werkzeuge zum Schutz von Software [56] auch noch im weiteren Verlauf dieser Arbeit als Quelle dienen, haben Methoden und Werkzeuge entwickelt, welche diese Aufgabe automatisiert erledigen. Grundsätzlich sind diese vergleichbar zu Code-Optimierern, wie sie jeder Compiler mitbringt, allein die Ziele differieren etwas: Minimierung der Laufzeit (oder des Platzbedarfes) auf der einen, Minimierung der Laufzeit sowie Maximierung der Entropie auf der anderen Seite. Generell arbeiten solche Programme auf drei Ebenen, um ihre Transformation durchzuführen:

- *Lexikalisch*: Auf Code-Ebene werden die Namen der Variablen und Bezeichner durcheinander geworfen. Dies ist sicherlich die schwächste Art der Obfuscation, doch trägt auch sie zu dem übergeordneten Ziel des Erschwerens von Reverse Engineering bei.

- *Strukturell*: Der Kontrollfluss des Programms wird um bedingte Verzweigungen erweitert, deren Werte und Ergebnisse dem Programmierer bekannt sind, vom Angreifer aber nur schwer nachvollzogen werden können. Diese *opaque predicates* verkomplizieren nach außen den Ablauf, während intern aufgrund ihrer festen Wahrheitswerte alles beim Alten bleibt.
- *Datenorientiert*: Auch die Art der Daten lässt sich verschleiern, um den Angreifer zu verwirren: Ein bool'scher Datentyp beispielsweise, der durch den Zustand zweier Integer repräsentiert wird, ist nicht mehr sofort als solcher zu erkennen. Die Quelle [56] bietet hierzu ein ausführliches Beispiel an.

Und auch wenn Stamp nicht ganz unkritisch bemerkt, dass die Code Obfuscation kein Allheilmittel sei und weit hinter den vor allem durch die Java-Gemeinde an sie gestellten Erwartungen zurückbliebe, trägt sie ihren Teil zum Ergebnis bei.

3.6.4 Software Unique-ification

Wie eingangs des Kapitels erwähnt, ist es auch Ziel des Sicherungs-Subsystems, die globale Sicherheit aller Instanzen des Systems unabhängig vom Status jedes einzelnen Systems zu machen. Wird die Sicherungsschicht in Instanz `A` überwunden, soll das keine Rückschlüsse auf das Wie des Überwindens in Instanz `B` zulassen.

Zu diesem Zweck muss jede Instanz ein gewisses Level an Einzigartigkeit mitbringen. Diese kann sich sowohl extern (sprich: Auf die Funktionalität des Systems) als auch rein intern (auf dessen Realisierung) auswirken, wobei externe Veränderungen zwar mehr Sicherheit, jedoch auch mehr Aufwand bedeuten: Ist beispielsweise der Verschlüsselungsalgorithmus jeder Instanz verschieden, so muss ein Inhalt eigens pro Instanz erstellt werden und wäre auch an diese gebunden, was zusätzlich auf Kosten der Interoperabilität ginge. Einzigartigkeit auf unterer Ebene hat mit dieser Problemklasse nicht zu kämpfen, während obiges Ziel trotzdem erreicht wird.

Methoden, welche aus jeder Instanz ein Unikat zu erzeugen versuchen, sind denen des Polymorphen Codes nicht unähnlich, allerdings wird hier Instanz eher im Sinne von "Kopie" des Systems verstanden: Das System von Benutzer `A` soll sich von Haus aus etwas von dem des Benutzers `B` unterscheiden, unabhängig davon, dass jeder Startvorgang des Systems eine etwas veränderte Variante hervorbringen könnte.

3.6.5 Tamper-Checking

Unter Tamper-Checking ist eine Funktionalität zu verstehen, welche zur Laufzeit des Systems überprüft, ob dieses sich in einem erwarteten, unangetasteten Zustand befindet. So soll gepatchtem, um Sicherheitsfunktionen erleichtertem Code auf die Schliche gekommen werden. Wird eine Veränderung des Programmcodes bemerkt, soll dieses zu Fehlfunktionen, beispielsweise Abstürzen, des Systems führen, welche seitens des Angreifers nicht notwendigerweise als Reaktion auf seine Attacken gedeutet werden müssen. Dieses Verhalten wird oft als *Fragilization* (Verwundbarkeit) bezeichnet: Eine geringe

Änderung kleiner Funktionen führt zu einem Fehlverhalten des gesamten Komplexes.

Collberg und Thomborson nennen zwei Ansätze, um Tamper-Checking zu realisieren:

- Den Vergleich der Struktur des zu untersuchenden Codes mit dem ursprünglichen anhand von Hash-Werten, welche beispielsweise mit dem MD5-Algorithmus berechnet wurden.
- Den Vergleich bestimmter Zwischenergebnisse im Programmfluss mit bekannten Soll-Werten, was auch als *Program/Result-Checking* bezeichnet wird.

Bei Anwendung dieser Maßnahmen innerhalb des Programms ist, wie bei allen sicherheitsrelevanten Aspekten, natürlich darauf zu achten, dass der entsprechende Code räumlich und zeitlich gut über das Gesamtprogramm verteilt ist, um dessen schnelle Detektion durch Angreifer zu vermeiden.

3.7 Das Wiedergabe-Subsystem: Frei sein oder nicht frei sein

Durch Anti-Debugging-Maßnahmen kann der Versuch unternommen werden, die entschlüsselten digitalen Daten vor dem Benutzer zu verbergen und vor seinen expliziten Zugriffen zu schützen. Spätestens bei der Wiedergabe der Inhalte aber soll der Anwender sehen, hören oder lesen können, zu was er laut Lizenz berechtigt ist. Das Wiedergabe-Subsystem kämpft nun mit dem Dilemma, einerseits diese generische Funktion eines Medien-Abspielgerätes sicherzustellen, aber trotzdem ein Optimum an Schutz auch über die digitale Verarbeitung hinaus gewährleisten zu müssen: Denn das erklärte Ziel des DRM bleibt, wie Stamp es formulierte, “persistenter Schutz, der dem Inhalt dauerhaft anhaftet”.

3.7.1 Watermarking und Fingerprinting

Die Technik des digitalen Wasserzeichnens soll diesem bleibenden Schutz zur Durchsetzung verhelfen, indem durch sie mittels steganographischer Verfahren unsichtbare Metainformationen in die Nutzdaten eingewoben werden. Jana Dittmann hat zu den theoretischen Grundlagen dieses weiten Feldes ein Standardwerk verfasst [57], welches unter [58] bereits zusammenfassend verarbeitet wurde. Hier soll deshalb nur der Grundgedanke anhand von Bild- und Audio-Signalen nachgezeichnet werden, obwohl die Technik sogar, wie Collberg und Thomborson verdeutlichen [56], auf ganze Softwaresysteme angewandt zu werden vermag:

Bild- wie Audiodaten lassen sich als Frequenzspektrum darstellen und speichern. Hierbei repräsentiert das niederwertigste Bit (Least Significant Bit) eines Blocks bestimmter Größe die höchste Frequenz des codierten Spektrums. Diese kann vom Menschen allgemein audiovisuell nicht mehr (beziehungsweise: kaum noch) wahrgenommen werden kann. Der Steganograph nutzt dieses LSB deshalb, um in ihm die Metainformationen zu verbergen. Je nach deren Inhalt und Nutzen unterscheidet man denn auch

- *Watermarking*: Die Metainformationen enthalten Angaben über den Rechteinhaber, um die Urheberschafft bei Streitigkeiten eindeutig klären zu können.
- *Fingerprinting*: Die Metainformationen enthalten Angaben über den Käufer oder Besitzer, um im Falle eines Auftretens illegaler Kopien diese zu der "undichten Stelle" zu Zwecken der Ahndung zurückverfolgen zu können.

Das große Problem des Watermarkings ist jedoch, dass es an der nötigen *Robustheit* noch entschieden hapert: Gängige Wasserzeichen lassen sich durch so einfache Tricks (hier am Beispiel eines Bildes) wie leichtes Drehen, Komprimieren oder Zerlegen in Teilbereiche meist irreparabel beschädigen, so dass der zu schützende Inhalt wieder "frei" wird. Auf der anderen Seite können zu robust generierte Markierungen durchaus wahrnehmbar hervortreten, was auch unerwünscht ist, da es den Wert des Inhalts schmälert. Neuere Forschungsergebnisse lassen jedoch Hoffnung erstehen: Den Fraunhofer Instituten für integrierte Publikations- und Informationssysteme (IPSI) und integrierte Schaltungen (IIS) ist es vor kurzem gelungen, die digitalen Markierungen von über analoges Radio ausgestrahlten Audiodateien nach deren Re-Digitalisierung erneut auszulesen [59].

3.7.2 "Anti Screen Capture" und weitere hardwarenahe Techniken

Um es jedoch gar nicht erst zum Datenklau kommen zu lassen, werden seitens der Industrie immer wieder Vorschläge eingebracht, welche die Sicherung der analogen "letzten Meile" zum Ziel haben. Meistens gehen sie in Form von Forderungen direkt bei den zuständigen politischen Stellen ein, um diese "*analog hole*" genannte letzte große Lücke ein für alle Mal und wiederspruchsfrei zu schließen. Einer der letzten Versuche dieser Art vor dem amerikanischen Senat nahm beinahe groteske Ausmaße an und wurde vehement bekämpft [60]:

Jeder Analog-Digital-Konverter solle, so die Eingabe, die von ihm erfassten Daten auf Legalität gemäß des Urheberrechts untersuchen und erst bei positivem Befinden eine Konvertierung zulassen. Es erfordert nicht viel Fantasie, das Nichtvorhandensein technischer Grundlagen und die Möglichkeit haarsträubender Ergebnisse zu erkennen.

Doch abseits dieser durchaus ernst gemeinten, jedoch nichtsdestotrotz skurril anmutenden Auswüchse, existieren durchaus realistische Ansätze auf diesem Gebiet, beispielsweise, um auf PC's einen Screenshot zu unterbinden oder das Abgreifen digitaler Signale an Grafik- oder Soundkarte zu verhindern. Diese Methoden müssen, um effektiv zu sein, jedoch ganz dicht auf der Hardware, zumindest jedoch auf der Kernelebene des zugrunde liegenden Betriebssystems aufsetzen, um ihren Zweck zu erfüllen. Das wiederum führt zu derart speziellen, plattformspezifischen Vorgehensweisen, dass eine vernünftige Abstraktion auf Allgemeines Niveau kaum zu finden zu sein scheint, weshalb das Thema an dieser Stelle nicht weiter vertieft werden soll.

4 Fazit

4.1 Bewertung

DRM – Technik die begeistert? Die eingangs gestellte Frage lässt sich nicht so leicht beantworten. Interpretiert man "begeistern" als "theoretisch fundiert und praktisch nutzbar sein", so lässt sich, zumindest für die das DRM aufspannenden Kerntechnologien, ein Ja zu dieser These finden. Doch das System als Ganzes? Sicherlich repräsentiert es mehr als die Summe der eingeflossenen Technologien, und in eine abschließende Bewertung muss deshalb auch eine Technologie-Folgen-Abschätzung mit einfließen:

Im zweiten Kapitel dieser Arbeit wurde auf diese Seiteneffekte des DRM-Ansatzes umfassend eingegangen. Vor allem kamen dort die manigfaltigen Bedenken ihm gegenüber zum Ausdruck. Dieses allein sollte jedoch noch keine Wertung darstellen. Vielmehr muss ein weitreichende Veränderungen bewirkendes System zuerst und vor allem kontrovers diskutiert werden, so dass, wenn alle Gegenargumente gehört und für lösbar (oder als untergeordnet) erachtet wurden, die Einführung guten Gewissens und unter Vergegenwärtigung der Folgen geschehen kann. Und es existieren durchaus gute Gründe, die Veränderungen rechtfertigen:

Wie bereits mehrfach anklang, ist unsere Zivilisation auf dem Weg zu einer Wissensgesellschaft, also auf dem Weg zu einer Form, in welcher "Wissen" (oder "Inhalt") als abstrakter Ausdruck für geistige Werke, den höchsten Wert genießt. Hierfür existiert in der Bevölkerung jedoch kaum Verständnis, denn digital repräsentierte Inhalte werden, wie gezeigt wurde, hemmungslos kopiert und verbreitet, ohne dass ein Sinn für deren Wert vorhanden wäre. Diese Einstellung ist wohl stark gebunden an die ressourcenverzehrlosen Möglichkeiten, mit digitalen Daten umzugehen. Nur, wenn hier ein Umdenken stattfindet, ein Wertschätzen im Sinne einer Bereitschaft, für Daten und Dienstleistungen im Bereich des Internets zu bezahlen, so wie man es in der analogen Realität als Selbstverständlichkeit erachtet, kann sich die schon angebrochene Entwicklung zu vermehrter digitaler Verarbeitung durchsetzen. Ansonsten ist sie vorweg zum Scheitern verurteilt.

DRM in der hier dargelegten Form könnte dieses Bewusstsein erschaffen, indem es Werte und Rechte in Bezug auf Inhalte zwangsverdeutlicht. Die dargelegten Techniken zum Erreichen dieses Zieles scheinen dieses in Aussicht zu stellen, auch wenn dieser Punkt in der Literatur oft anders bewertet wird [61]: Mit den gegebenen Rechtsmitteln ausgestattet, sollte es einem System möglich sein, und hier schließt sich der aus der Begriffsdefinition gespannte Bogen, hinreichende Sicherheit im Sinne von "nicht unüberwindbar, jedoch praktisch sicher und die Illegalität von Angriffen verdeutlichend" zu bieten. Als praktisch sicher mag dabei in Analogie zur Kryptologie gelten, was Schmitt in [39] definiert.

Das Problem scheint also nicht in unzulänglicher Technik begründet zu sein. Des weiteren wurde deutlich, dass es ebenso wenig in der aus Bequemlichkeit und falschem Sparwillen entstandenen Abneigung vieler Benutzer dem DRM gegenüber zu suchen ist, denn diese Sichtweise muss sich den geänderten Anforderungen eines neuen Medien-

zeitalters unterordnen, wohlbemerkt nicht zum Schlechten, sondern zum Anderen hin. Das Problem ist vielmehr folgendes: DRM ist als totalitäres System ausgelegt, es soll per Definition und Wunsch der Initiatoren vollkommene Kontrolle über die schützenswerten Daten liefern. Auch wenn diese Stärke des Schutzes zumindest noch eine Weile auf sich warten lassen wird, wirft dieser Sachverhalt Bedenken an dem grundsätzlichen Ansatz auf: Zu schmerzlich sind Erinnerungen an menschliches Hegemonialstreben und Machtmissbrauch auf anderen Feldern, als dass hier ein potentiell missbräuchlich zu verwendendes Instrument diesen Ausmaßes auf den Weg gebracht werden sollte. Und auch abseits dieses "worst case" sind die Datenschutzrechtlichen Bedenken groß. Es sollte also mehr Weitblick an den Tag gelegt werden, als nur auf eine "Wende zum Guten" [62] dessen zu hoffen, was bereits den Startlöchern entsprungen ist.

Vielleicht sollte man sich die Weisheit des Predigers [63] zu Eigen machen, der schon vor langer Zeit, damals jedoch in anderem Kontext, zu einem Weg der Mitte aufrief, und weniger polarisierenden Systemen den Vortritt lassen. Denn mit "Light Weight DRM" [64] geht eine Entwicklung an den Start, welche die Handhabung von Rechten im analogen Umfeld auf das Digitale zu übertragen sich anschickt und somit eine flexiblere Ausgestaltung des Schutzes verspricht. Solchen Systemen, Praxistauglichkeit vorausgesetzt, könnte die Zukunft gehören, stellen sie doch einen gangbaren Kompromiss zwischen Hersteller- und Konsumentenwünschen dar:

4.2 Ausblick

Der "Light Weight Digital Rights Management"-Ansatz des Fraunhofer Institutes für Integrierte Schaltungen möchte eine Handhabung digitaler Inhalte im Bereich des "fair use", ähnlich dem heutigen Ansatz in der Welt der Printmedien, implementieren: Ein Benutzer darf seine Inhalte überall hin kopieren, solang er sie mit seiner persönlichen Signatur abzeichnet. Sollten seine Medien jedoch in die breite Öffentlichkeit durchsickern, kann er dafür zur Rechenschaft gezogen werden. Die Verantwortung liegt also mit auf Seiten der Benutzer.

Um dem Misstrauen vor Zertifizierungsstellen gerecht zu werden, soll es überdies drei unterschiedliche Benutzungs-Level geben, zu deren Realisierung es zwei verschiedenen Dateiformate, ein maschienengebundenes sowie ein freies, signiertes, geben soll:

- Stufe 1: Der Benutzer kann heruntergeladenen Inhalte auf dem ursprünglichen System wiedergeben
- Stufe 2: Der Benutzer kann neue Inhalte selbst erstellen, um sie auf dieser Maschine abzuspielen
- Stufe 3: Alle maschinengebundenen Inhalte können nun weitergegeben werden, wenn sie signiert wurden. Nur hierfür muss sich der Benutzer bei einer "Certification Authority" (CA) seiner Wahl registrieren.

Natürlich bietet auch diese Herangehensweise an die DRM-Thematik genügend Ansätze für kritische Diskussion: Registrierung, Daten-Tracking und alle damit verbundenen Datenschutzrechtlichen Bedenken existieren auch hier, und prinzipiell ähneln sich

die verwendeten Techniken sehr, was schlussendlich auch ähnliche Verwendungsweisen nahelegt. Doch der Ansatz gestaltet sich weniger restriktiv, weniger totalitär als vorherige Vorschläge, und es wohnt einem Kompromiss nun einmal inne, dass auf beiden Seiten Abstriche zu machen sind.

Die endgültige Antwort wird jedoch auch weiterhin Gegenstand vieler Diskussionen bleiben und kann hier nicht gegeben werden. Was bleibt, ist nur die grundsätzliche Einschätzung des Systems als für die gestellte Aufgabe durchaus gewappnet sowie die Warnung vor dessen darüber hinaus weit reichenden Konsequenzen. Durch vermehrte Aufklärungsarbeit unter allen Beteiligten – Anbietern, Konsumenten wie auch Technikern – wird ein Konsens jedoch wahrscheinlicher. Es besteht Hoffnung, hierdurch dazu beigetragen zu haben.

Literatur

[1] Gerald Himmelein, “Ganz im Vertrauen: TCPA ist tot, es lebe die TCG” *c't Magazin für Computer Technik* 9/2003: 52

[2] Joerg Heidrich, “Kopieren verboten?”, *c't Magazin für Computer Technik* 9/2003: 20

[3] Richard Sietmann, Stefan Krempl, “Zaghaft nach Digitalien: Das neue Urheberrecht auf Probe”, *c't Magazin für Computer Technik* 9/2003: 18-20

[4] Dr. Ingolf Prinz, “Musikkonserven mit Paragraphensauce: Kopiergeschützte Tonträger, Abspielhemmnisse und private Kopie”, *c't Magazin für Computer Technik* 7/2003: 150

[5] Prof. Dr. Francesco P. Volpe, David Bär, “Die Un-CDs: So arbeiten Abspielsperren für Audio-CD's”, *c't Magazin für Computer Technik* 7/2003: 144-149

[6] Christian Wenz, “Ohren auf den Schienen: Umgehungsmöglichkeiten für DRM-Schutzmechanismen”, *c't Magazin für Computer Technik* 6/2003: 238

[7] Tobias Hauser, “Finger weg: DRM-Systeme in der Praxis”, *c't Magazin für Computer Technik* 6/2003: 234-237

[8] Sven Hansen, Dr. Volker Zota, “Kaufrausch versus Tauschrausch”, *c't Magazin für Computer Technik* 6/2003: 144-145

[9] Gerald Himmelein, “Ganz im Vertrauen: Neues aus der Welt des Trusted Computing”, *c't Magazin für Computer Technik* 6/2003: 40

[10] Richard Sietmann, “'Gegenpositionen aufbauen': Der Weltgipfel für die Informationsgesellschaft nimmt Konturen an”, *c't Magazin für Computer Technik* 5/2003: 54-55

[11] Holger Bruns, “Wissensgesellschaft in der Diskussion”, *c't Magazin für Computer Technik* 5/2003: 34

[12] Richard Sietmann, “An der Klagemauer: Urheberrechts-Novelle: Klare Fronten, aber keine Alternativen”, *c't Magazin für Computer Technik* 4/2003: 20-21

[13] Peter-Michael Ziegler, “MS-E-Books schutzlos”, *c't Magazin für Computer Technik* 2/2003: 28

[14] Brian Kahin, “Auf dem Holzweg: was läuft schief in der Politik zum 'geistigen Eigentum'?”, *c't Magazin für Computer Technik* 1/2003: 74-79

[15] Janko Röttgers, “'Wir brauchen offene Systeme': Howard Rheingold über die soziale Revolution durch Mobiltechniken”, *c't Magazin für Computer Technik* 1/2003: 72-73

[16] Michael Plura, “Entmündigung des PC-Besitzers: Lucky Green, US-amerikanischer Kryptoexperte, über die von TCPA und Palladium ausgehenden Gefahren”, *c't Magazin für Computer Technik* 26/2002: 58-59

[17] Michael Plura, “Sicherheit und Vertrauen: Thomas Rosteck, Leiter des Product Marketing für Sicherheits-ICs bei Infineon, über die Technik und Vorzüge von TCPA”, *c't Magazin für Computer Technik* 26/2002: 56-57

[18] Michael Plura, “Schlossgespenst: hat TCPA auch positive Seiten für den Anwender?”, *c't Magazin für Computer Technik* 26/2002: 54

[19] Michael Plura, “Der PC mit den zwei Gesichtern: TCPA und Palladium - Schreckgespenster oder Papiertiger?”, *c't Magazin für Computer Technik* 24/2002: 186-188

[20] Richard Sietmann, “Wissen ist Geld: Urherberschutz, 'Geistiges Eigentum' und die Rechteverwerter”, *c't Magazin für Computer Technik* 24/2002: 108-117

[21] Michael Plura, “Der versiegelte PC: Was steckt hinter TCPA und Palladium?”, *c't Magazin für Computer Technik* 22/02: 204-207

[22] Dirk Günnewig, Tobias Hauser, “Musik im Hochsicherheitstrakt: Digital Rights Management - Stand der Dinge”, *c't Magazin für Computer Technik* 16/2002: 182-185

[23] Mark Stamp, *Mark Stamp's CV*, 24.03.2003, <http://home.earthlink.net/ ~mstamp1/mss_v.html>

[24] Mark Stamp, *Digital Rights Management: The Technology Behind the Hype*, 19.12.2002, Department of Computer Science, San Jose State University, 05.03.2003, <http://home.earthlink.net/~mstamp1/papers/DRMpaper.pdf>

[25] Renato Iannella, *Curriculum Vitae for Renato Iannella*, 15.10.2002, 08.04.2003, <http://renato.iannella.it/cv/index.html>

[26] Renato Iannella, “Digital Rights Management (DRM) Architectures”, *D-Lib Magazine*, Volume 7 Number 6, Juni 2001, 07.04.2003, <http://www.dlib.org/dlib/june01/iannella/06iannella.html>

[27] Margarita A. Kousseva, *Digital Rights Management: Literature Review*, 06.12.2002, School of Computer and Information Sciences, Nova Southeastern University, 24.03.2003, <http://www.nova.edu/~kousseva/literature_review.html>

[28] Ulrich Dieter Einbrodt, *Legale MP3-Downloads: Musik 2. Klasse oder geniale Anwendung neuer medialer Distributionsmärkte? Das Beispiel MP3.com*, 1999, 27.02.2003, <http://bibd.uni-giessen.de/ghtm/1999/uni/p990010.htm>

[29] Ulrich Dieter Einbrodt, *The Juxtaposition of Good and Bad or: Legal and Illegal Downloads. The MP3 Format and its Chances for Musicians and Fans*, 2001, 27.02.2003,
<http://bibd.uni-giessen.de/ghtm/2001/uni/p010002.htm>

[30] *Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft*, Drucksache 15/38 des Deutschen Bundestages (15. Wahlperiode) vom 06.11.2002, 23.04.2003,
<http://dip.bundestag.de/btd/15/000/1500038.pdf>

[31] Florian Weis, Christian Albrecht, *Digital Rights Management*, Semesterarbeit an der Technischen Fachhochschule Berlin, Dezember 2002, 27.02.2003,
<http://www.tfh-berlin.de/˜godberse/semesterarbeiten/ ia2/drm.pdf>

[32] Judie Mulholland, *Digital Rights (mis)Management*, Position Paper for the W3C DRM Workshop, 23.01.2001, 27.02.2003,
<ttp://www.w3.org/2000/12/drm-ws/pp/fsu-mulholland.html>

[33] Austin Russ, *Digital Rights Management Overview*, The SANS Institute, 26.07.2001, 27.02.2003,
<http://www.sans.org/rr/securitybasics/rights.php>

[34] *Art & Commerce in the Digital Decade: Protecting intellectual property will take cooperation and innovation*, 03.06.2002, Microsoft Corporation, 01.04.2003,
<http://www.microsoft.com/issues/essays/2002/06-03digitalrights.asp>

[35] *Richard M. Stallman - List of Achievements and Awards*, 18.10.2002, Free Software Foundation, Inc., 01.04.2003,
<http://www.gnu.org/doc/Stallmanawards.html>

[36] Richard M. Stallman, Joshua Gay (Hrsgb.), "Words to avoid", *Free Software, Free Society: Selected Essays of Richard M. Stallman*, Philosopy of Software Freedom Series, GNU Press Oktober 2002, 01.04.2003 online unter
<http://www.gnu.org/philosophy/words-to-avoid.html>

[37] *23 – Nichts ist wie es scheint*, Ein Film von Hans-Christian Schmid, beruhend auf den wahren Begebenheiten um den Tod des Hackers Karl Koch im Jahr 1989, Buena Vista International, 1998, siehe auch (17.05.2003)
<http://www.moviesite.de/kritik.cfm?id=31>

[38] Tim Gerber, "Wunschkonzert", Editorial zum *c't Magazin für Computer Technik* 04/2003: 3

[39] Prof. Dr. W. Schmitt, Scriptum zur Lehrveranstaltung *Datensicherheit* im Sommersemester 2002 an der FH Giessen-Friedberg, 10.03.2001

[40] Diana Kelley, *Authentication as the Foundation for eBusiness*, Security Technology for Safewww Inc., 15.11.2001, 29.04.2003,
<http://www.securityfocus.com/infocus/1513>

[41] Mark Vandenwauver, Rene Govaerts, Joos Vandewalle, *Overview of Authetication Protocols*, 29.04.2003,
<https://www.cosic.esat.kuleuven.ac.be/sesame/papers/carnahan.pdf>

[42] *Authentication & Authorization: Complementary Solutions for Securing the Digital Enterprise*, 01.07.2001, BioNetrix Corporation, 29.04.2003,
<http://www.bionetrix.com/pdf/Netegrity.pdf>

[43] Microsoft .NET Passport, global Einheitlicher Authentikationsdienst (nicht nur) für DRM, 05.05.2003,
<http://www.passport.net>

[44] Andrew Conry-Murray, *Emerging Technology: Microsoft's Passport to Controversy*, 03.04.2002, 06.05.2003,
<http://www.networkmagazine.com/article/NMG20020304S0003>

[45] Renato Iannella, *Open Rights Language Requirements*, ISO/IEC JTC1/SC29/WG11 M6974, März 2001, 06.05.2003,
<http://www.iprsystems.com/MPEG/m6974.pdf>

[46] Renato Iannella, *Open Digital Rights Language (ODRL)*, Version 1.1 08.08.2002, 06.05.2003,
<http://odrl.net/1.1/ODRL-11.pdf>

[47] *Open Digital Rights Language: A Rights Expression Language for Digital Asset Management and E-Commerce*, Informationsbroschüre der ODRL Initiative, 06.05.2003,
<http://odrl.org>

[48] *XrML 2.0 Technical Overview*, Version 1.0 08.03.2002, 15.04.2003,
<http://www.xrml.org/reference>

[49] *XrML 2.0 Specifications*, Spezifikationen und Beispiele zum XrML-Standard 2.0, nach Registrierung per eMail anforderbar (15.04.2003) unter
<http://xrml.org>

[50] Prof. Dr Franck Leprevost, Prof. Dr Bertrand Warusfel, *Security Technologies for Digital Media*, Final Report to the European Parliament Directorate-General for Research, Directorate A, STOA Programme, Mai 2001, 29.04.2003,
<http://www.europarl.eu.int/stoa/publi/pdf/00-06-01_en.pdf>

[51] Inbar Raz, *Anti Debugging Tricks*, 05.03.2003,
<http://www.geocities.com/angel-miguel/tutdown/antidebug.htm>

[52] SnakeByte, *Polymorphe Viren*, 24.03.2003,
<http://www.snake-basket.de/d/poly.txt>

[53] Nightmare Joker, *How to Encrypt Wordbasic and VBA Code*, 23.03.2003,
<http://vx.netlux.org/texts/html/m6t.html>

[54] Thomas Klausner, *Eine Einführung in Obfuscation mit Perl*, Linuxwochen 2002, 30.06.2002, 23.03.2003,
<http://domm.zsi.at/talks/obfu_linuxwochen/obfu_lw.html>

[55] Gregory Wroblewski, *General Method of Program Code Obfuscation*, 2002, 08.05.2003,
<http://www.mysz.org/papers/obfuscation.ps.gz>

[56] Christian S. Collberg, Clark Thomborson, "Watermarking, Tamper-Proofing, and Obfuscation – Tools for Software Protection", *IEEE Transactions on Software Eengineering*, Vol. 28, No. 8, August 2002, 25.03.2003,
<http://www.cs.auckland.ac.nz/čthombor/Pubs/01027797a.pdf>

[57] Jana Dittmann, *Digitale Wasserzeichen*, Springer-Verlag Berlin Heidelberg New-York 2000, ISBN 3-450-66661-3

[58] Sven Hlawatsch, *Digital Watermarks*, Seminararbeit an der FH-Giessen, 12.05.2003,
<http://homepages.fh-giessen.de/ hg10013/>

[59] "Digitale Wasserzeichen in Hörfunksendungen" Heise Newsticker, 31.01.2003, 12.05.2003, <http://heise.de/newsticker/data/anw-30.01.03-006/default.shtml>

[60] *Hollywood wants to plug änalog hole,regulate A-D converters*, Beitrag im Newsarchiv des Förderverein Informationstechnik und Gesellschaft e.V., 24.03.2002, 23.03.2003,
<http://www.fitug.de/news/horns/old/newsticker240502192617.html>

[61] Hannes Federrath, *Scientific evaluation of DRM systems*, 28.03.2003,
<http://page.inf.fu-berlin.de/feder/drm/>

[62] Sabrina Ehlers, *Proseminar: Sicherheitskonzepte im Internet*, Proseminararbeit an der Universität Tübingen, Lehrstuhl für Rechnerarchitektur, im Sommersemester 2002, 05.05.2003,
<http://www-ra.informatik.uni-tuebingen.de/lehre/ss02/
pro_sicherheit_ausarbeitung/proseminar_ehlers_ss02.pdf>

[63] *Die Bibel* in der Übersetzung Martin Luthers, Buch des Predigers, Kapitel 7, Verse 16-18

[64] *LWDRM(r) - Light Weight Digital Rights Management*, Fraunhofer Institut für Integrierte Schaltungen, 05.03.2003,
<http://www.iis.fraunhofer.de/amm/techinf/ipmp/>