

# Digital Restrictions Management als Konterrevolution im Cyberspace

Volker Grassmuck  
Kollegiatentag der SEL Alcatel Stiftung  
Schloß Reichenow, 7.-8. Februar 2003

Heute ist der Cyberspace durch eine offene Architektur gekennzeichnet. IBM veröffentlichte die Spezifikationen seiner PC-Architektur. Das führte schnell zu Nachbauten oder Clones und damit zu einer Senkung der Preise. Die einheitliche Plattform von „IBM-Kompatiblen“ beförderte die Innovation und erhöhte die Auswahl für die Käufer. Ebenso offen sind Architektur und Protokolle des Internet. Auch dieses stellt eine gemeinsame Plattform für Hard- und Software-Innovationen jeder Art dar.

Morgen wird diese offene Architektur im Namen des Urheberrechts bis zu den Betriebssystemen, Gerätetreibern und der Hardware in eine proprietäre Kontrollinfrastruktur verwandelt sein.

*„It's a funny thing,“ says Bill Gates. „We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains.“ For instance, Palladium might allow you to send out e-mail so that no one (or only certain people) can copy it or forward it to others. Or you could create Word documents that could be read only in the next week. In all cases, it would be the user, not Microsoft, who sets these policies. (Levy 2002)*

Das Palladium-FAQ von Microsoft bestätigt diesen Strategieschwenk: „Anyone can impose access control over remote networks and/or enforcement of user policy over sensitive information.“

Stellen Sie sich eine Welt von allgegenwärtigen DRM-Systemen vor. In ihr würde jede Software DRM-Funktionen verwenden. Jedes Textverarbeitungsprogramm, jeder Editor für die Fotos und Videos aus Ihren DigiCams, jeder Mailer würde Sie vorm Speichern oder Verschicken fragen, welche digitalen Nutzungsrestriktionen Sie ihren Daten auferlegen wollen. Ihnen bliebe also gar keine Wahl, als Ihren „Content“ rechtetechnisch als Ihr Eigentum zu beanspruchen.

Was bedeutet diese Vision? Technologisch: eine flächendeckende und lückenlose Kontrollinfrastruktur, bis in die Kapillargefäße des Cyberspace hinein. Rechtlich: ein Sonderschutz gegen die Umgehung von DRMs, bei -- im Internet vollständiger -- Aufgabe eines gesellschaftlichen Interessenausgleichs. Im Effekt bedeutet die aktuelle Novelle des Urheberrechtsgesetzes die Übergabe der Gestaltungskompetenz über den Cyberspace vom gewählten Gesetzgeber an die Medienkonzerne.

Für die Datenherren der Unterhaltungsindustrie wäre das das Schlaraffenland. Einen vergleichbaren Strom von hochauflösenden, individualisierten Nutzungsdaten gab es noch nie. Auch andere könnten offensichtlichen Nutzen aus der Kontrolle über „sensitive Informationen“ ziehen.

Die Church of Scientology setzt das Urheberrecht ohnehin schon systematisch ein, um Kritiker zum Schweigen zu bringen. Im vergangenen Jahr erwirkte die Sekte z.B. im Namen des Urheberrechts die Löschung von Sektenkritikern aus der Google-Datenbank. Per DRM könnte sie ihre internen

Dokumente gegen Zugriff viel effektiver sperren. Eine kritische Berichterstattung, investigativer Journalismus, Whistle Blowing von Betroffenen und Angehörigen über die Sekte wären damit vereitelt. Auch Microsoft wäre sicher für ein Verfahren dankbar gewesen, hausinterne eMails, die im Kartellverfahren zu Beweismitteln wurden, per Fernbedienung oder Zeitschaltung zu eliminieren.

Doch der eigentliche Schachzug von Gates ist es, DRM von einem Kontrollinstrument der Datenherren zu einem Werkzeug für jedermann umzudefinieren. Er gewinnt damit möglicherweise sogar Akzeptanz. Es sieht gut aus, wenn nicht nur einige multinationale Informationskonzerne an den Hebel sitzen, sondern jeder ein kleines Hebelchen in die Hand bekommt. Nicht, dass Normalsterbliche irgendetwas dabei zu gewinnen hätten. Aber die hat der Monopolist ohnehin in der Tasche. Natürlich geht es in erster Linie darum, die Datenherren zu überzeugen, ihre Inhalte in Microsofts Formaten zu verkaufen. Konkurrenz hat es dabei nur noch von Apples Quicktime und von Real Networks. Letzterem beschied ein DRM-Branchendienst vor kurzem ([www.drmwatch.com](http://www.drmwatch.com), 9.1.03) eine gewisse Überlebenschance aufgrund besserer Technologie, besserer Server-Skalierbarkeit und aufgrund von Hollywoods Mißtrauen gegen Microsoft. Da AOL-Time-Warner Real unterstützt, wähnt man sich in einer Neuauflage des Browser-War.

Medienpraktisch oder, wenn Sie so wollen, informationsökologisch bedeutet diese Entwicklung, dass wir Nutzungseinschränkungen auf privaten Homepages, in Newsgroup- und Mailinglisten-Postings sehen werden. Immer größere Teile des Netzes werden für Suchmaschinen unsichtbar. Und wenn erst noch Abrechnungsdienste für jedermann dazukommen, wird es kein Halten mehr geben.

Vor allem aber wird uns eine solche Architektur des Cyberspace beibringen, infokapitalistisch zu denken. Gates modelliert die Welt nach seinem Ebenbild. Was bislang auf kommerzielle Unterhaltungsdaten beschränkt war, wird auf jede beliebige digitale Äußerung ausgeweitet. Damit wird uns beigebracht, von unseren Urlaubsfotos, unseren Seminararbeiten, unseren Mailinglisten-Postings als „geistiges Eigentum“, als „Content“ und als potentielle Ware zu denken. Das „Volks-DRM“ führt zu einer Ver-Copyright-ung der gesamten Wissensumwelt.

## Das Großprojekt DRM

*Digital Rights Management (DRM) is the umbrella term for new business processes designed to unleash the tremendous capabilities of the Internet.* (InterTrust)

*A more favorable way to look at trusted systems is to compare them to vending machines.* (Mark Stefik, "Letting Loose the Light" 1996, S. 13)

Zunächst zur Bezeichnung „Digital Rights Management“. Die Verkürzung von „Copyrights“ zu „Rights“ suggeriert, dass es nur eine Art von Rechten im Digitalraum gäbe, dass allein die Verwerter urheberrechtlich geschützter Werke über digitale Rechte verfügen. Unterschlagen wird -- und zwar nicht nur rhetorisch, sondern ganz praktisch durch technische Mittel --, dass auch Bürger Rechte im Cyberspace haben, z.B. das auf digitale Unverletzlichkeit der Wohnung, auf Datenschutz und das auf Teilhabe am kulturellen Leben durch Zugang zu veröffentlichten Werken in Bibliotheken und durch die Privatkopie (Art. 5 GG).

Genauer wäre daher die Version von Richard Stallman, der empfiehlt, von „Digital Restrictions Management“ zu sprechen (Stallman, Words to Avoid). Das trifft präzise den ökonomischen Sinn von DRM: In einer Informations-Umwelt, die keinen Mangel kennt, durch Nutzungsrestriktionen Mangel zu erzeugen, um dann seine Behebung als Dienstleistung verkaufen zu können. Haben wir beim Buch- oder Schallplattenhändler sämtlich privat möglichen Nutzungsformen erworben, erlaubt die Technik, Zahl oder Zeit der Wahrnehmungen, Kopieren, Verleihen, Weiterverkaufen usw. zu unterbinden und einzeln zu verkaufen.

Den Kern der technokratischen Vision von DRM bildet also Technologie, die den Umgang mit Wissen kontrollierbar macht. Doch wo werden ihr Grenzen gesetzt? Wird sich die vom Gesetzgeber abgesicherte „technologische Selbsthilfe“ der Datenherren auf legitime Interessen von Urhebern und Mittlern beschränken oder wird sie den digitalen Kommunikations- und Wissensraum für alle anderen Zwecke als das Verkaufen von digitalen Waren unbrauchbar machen? Worin begründet sich ein Verbot derselben technologischen Selbsthilfe für ebenso legitime Interessen von Informations-Nutzern? Und vor allem: wer entscheidet? Es geht also darum, ob aus der zunehmenden wechselseitigen Durchdringung von Cyberspace und Gesellschaft eine Volksherrschaft entsteht oder ob Digitalien -- dieses Land, in dem wir alle in zunehmendem Maße leben, arbeiten, lernen und lehren, kommunizieren, uns amüsieren -- zu einem privat regierten Kommerzraum wird, in dem nicht demokratische Gesetze gelten, sondern Hausregeln. Es geht um die Macht.

DRM ist Zugangskontrolle zum Ausschluß aller nicht-autorisierten Nutzer und Nutzungskontrolle für autorisierte Nutzer, bei der DRM kontrolliert wer, was, wann, wo auf welche Weise nutzt.

In der Geschichte von DRM kann man vier Generationen oder Paradigmen unterscheiden:

1. Statische Stand-Alone Systeme (Objekt und Player)
2. Dynamische Systeme: Widerrufung und Systemerneuerung
3. Secure Boot
4. Krypto-Infrastruktur

### **1. Statische Stand-Alone Systeme (Objekt und Player)**

Am Anfang standen lokale Lösungen wie Kopierschutzverfahren für Computerprogramme (Dongle, Verschlüsselung, Standardabweichungen bei Diskettenformaten) und in der Unterhaltungselektronik z.B. Zugangskontrollen für Settop-Boxen für Satelliten- und Kabelempfang (Pay-TV)

Die ersten Geräte auf dem Konsumentenmarkt, die digitale Aufzeichnungen ermöglichten, waren DAT-Rekorder. Mitte der 1980er war die Technologie ausgereift, doch Philips und Sony führten sie nur mit gebremster Kraft auf dem Markt ein, denn inzwischen ging die Musikindustrie auf die Barrikaden. Der technologische Kompromiß, der bei diesen Auseinandersetzungen herauskam, war das *Serial Copy Management System* (SCMS). Da man bei einem Rekorder schlecht verhindern kann, dass er Daten speichert, sollte das SCMS wenigstens das Kopieren von Kopien verhindern. Die Technologie wurde rechtlich flankiert durch den *Audio Home Recording Act* (AHAR) von 1992. Diese Novellierung des US-Copyright Law verpflichtet alle Hersteller und Importeure von Geräten für digitale Audioaufnahmen, diese mit einem SCMS auszurüsten. Gleichzeitig verbietet sie Geräte, deren primärer Zweck es ist, solche Kopierschutzmechanismen zu umgehen, zu entfernen oder zu deaktivieren. Diese Regulierung einer Einzeltechnologie ist das Vorbild für

die generelle und weltweite Disziplinierung des Cyberspace im Namen des Urheberrechts, die wir derzeit erleben. Ein Kontrollstandard für eine neue Mediengeneration wird erarbeitet. Da der Markt ihn freiwillig nicht implementieren würde, schreibt der Gesetzgeber es ihm vor (vgl. die Hollings-Bill). Und da die Technologie unwirksam ist -- nur Tage nach der Markteinführung von SCMS fanden sich in einschlägigen Quellen Bauanleitungen, um es auszuschalten -- verbietet man auch ihre Umgehung.

Auch das Portable Document Format (PDF) stellt eine lokale Lösung dar, die nur Daten und Darstellungssoftware betrifft. 1993 von Adobe vorgestellt, erlaubt PDF standardmäßig, einzelne Nutzungen (Drucken, Ausschneiden, Verändern) zu verhindern und das Dokument mit einem Passwort zu schützen, und sie bietet eine Schnittstelle für DRM-Verfahren von Drittanbietern an. PDF ist heute eines der am weitesten verbreiteten DRM-Formate.

## **2. Dynamische Systeme: Widerrufung und Systemerneuerung**

Seit Ende der 1990er hält DRM-Technologie Einzug in sämtliche Geräte (Fotokopierer, Scanner, Festplatten, Satelliten-Dekoder, CPU), Medien (CD, Rundfunksignale, Dateiformate) und Software (Viewer, Editoren, Betriebssysteme), die mit urheberrechtlich geschütztem Material in Berührung kommen könnten. Von lokalen Systemen entwickeln sie sich zu solchen an der langen Leine des Netzes. Die heutigen DRM-Systeme, die auch als zweite Generation bezeichnet werden, sind ein komplexes dynamisches Gefüge aus unterschiedlichsten Ebenen und Bausteinen, die sowohl online wie offline zum Einsatz kommen.

(Überblicksdarstellungen in Bechtold 2002, European Commission 2002, Grassmuck 2002)

### **Objekt-Identifikation und Verschlüsselung: Was?**

Um feststellen zu können, worum es sich bei einer gegebenen Datei handelt, werden ihr Informationen über den Inhalt, die Künstler und die Rechteinhaber beigelegt. Dazu braucht es weltweit einheitliche Nummerierungssysteme nach der Art der ISBN für Bücher und des ISRC für Tonträger. Hier engagieren sich vor allem die Verwertungsgesellschaften, deren Abrechnung die Identifikation der genutzten Werke erfordert. Ihr Dachverband CISAC (*Confédération Internationale des Sociétés d'Auteurs et Compositeurs*) entwickelt nicht nur einzelne Nummernsysteme wie den *International Standard Works Code* (ISWC) für Kompositionen und die *International Standard Audiovisual Number* (ISAN) für Filme, die sich beide in der ISO-Standardisierung befinden, sondern mit dem *Common Information System* (CIS) auch ein *One-Stop Clearing-House* für Rechtfragen.

Speziell für Werke im Netz entwickelt die Printverlagsindustrie den *Digital Object Identifier* (DOI). Er soll eine automatisierte Rechteverwaltung von der Inhalterzeugung über Marketing und Vertrieb bis zur Nachkontrolle beim Käufer möglich machen. Er besteht aus Kennung, Metadaten und einem Namespace (fungiert auch als URI, der auf URLs, lokale Adressen, Standorte in Bibliothek usw. zeigen kann).

Neben einer solchen expliziten Kennzeichnung von Werken kann der Inhalt selbst sich auch durch seinen Fingerabdruck zu erkennen geben. Für die *AudioID*, die am selben Fraunhofer Institut entwickelt wurde, aus dem MP3 stammt, wird aus einem Musikstück eine kompakte, einzigartige Signatur errechnet und in einer Datenbank abgelegt. Spielt man dem System dann einen Ausschnitt aus einem unbekanntem Stück vor, wird daraus ebenfalls ein Fingerabdruck generiert und mit

der Datenbank abgeglichen. Bei einem Treffer meldet das System alle damit verbundenen Informationen. Die Wiedereerkennung funktioniert sogar, wenn man ihm ein Musikstück über ein Mobiltelefon vorspielt. Das experimentelle System schickt dann eine SMS mit Titel, Interpret und Bestellinformation zurück. Das System kann außerdem Radiokanäle abhören, um den Urhebern ihre Vergütung zu sichern, und helfen, nichtautorisierten Musik im Netz ausfindig zu machen.

Die eigentliche Zugangskontrolle beruht auf einer kryptographischen Kapselung der digitalen Objekte, die ausschließlich unter den Bedingungen geöffnet wird, die die Rechteinhaber festgelegt haben. Sicherheitsexperten sind der einhelligen Ansicht, dass Software-gestützte Kryptosysteme ernsthaften Angreifern grundsätzlich nicht standhalten können (z.B. Pfitzmann et al. 2002), daher geht der Trend zu einer Implementierung in Hardware. Ein Prozessor, z.B. auf einer Chipkarte, kann mit mechanischen, elektrischen und chemischen Mitteln gegen Manipulation gesichert werden.

Kryptosysteme bedürfen weiterer Mechanismen für die Schlüssel- und Transaktionsverwaltung und die Authentifizierung mit Hilfe digitaler Signaturen. Sie überschneiden sich daher mit vielfältigen anderen Einsatzbereichen wie Gewährleistung von Systemsicherheit, Vertraulichkeit und Datenschutz, Datenintegrität und Identitätsnachweis.

### **Subjekt-Identifikation: Wer?**

Ging es eben um die Kennzeichnung des Schutzgegenstands, so hier um die Kennzeichnung des Nutzers. Sie wird heute oft als Kopplung an eine Player- oder Hardware-ID realisiert. Dies erschwert jedoch die Übertragung z.B. auf portable Geräte. Daher geht der Trend generell zu einer personengebundenen Kodierung. Über eine Online-Registrierung jeder Kopie kann eine Person sich die gesetzlich zulässige begrenzte Zahl von Kopien einer CD für Auto, Schlafzimmer, Sicherung oder einer MP3-Datei für verschiedene Geräte anfertigen. Die Werke und ihre Nutzer hängen dann an der langen Leine eines zentralen Servers.

Für den Identitätsnachweis lassen sich z.B. Biometrie-Module einsetzen. Sony hat gerade einen Fingerabdruck-Leser im Memory Stick-Format vorgestellt (der somit in allen Vaio-Rechnern, Digitalkameras und digitalen Musikabspielgeräte der Firma einsetzbar ist).

Für das „Identitäts-Management“ kommt Microsofts Passport (das vor einer Woche Auflagen der EU Kommission zur Anpassungen an das europäische Datenschutzrecht erhalten hat, die Microsoft in den nächsten Monaten vornehmen will) oder das konkurrierende System der von Sun Microsystems angeführten Liberty Alliance zum Einsatz kommen.

Auch die Kopplung der ausgelieferten Daten mit dem Abrechnungsmechanismus ist ein wirksames Verfahren, denn ein Käufer wird das Werk kaum zusammen mit seinem Schlüssel an Dritte weitergeben, da diese damit auf seine Rechnung weitere Produkte kaufen könnten.

Digital World Services (DWS), die DRM-Tochter von Bertelsmann, nennt ihre Lösung den *Rights Locker*. Verkaufen Content-Anbieter ihre Online-Waren durch dieses System, werden die jeweils erworbenen Nutzungsrechte automatisch im persönlichen „Rechteschließfach“ registriert. Als Vorteil für den Kunden wird die Backup-Funktion angepriesen: Wenn die Festplatte stirbt, hat er immer noch seine Rechte im Netz und kann sich die Musikstücke usw. erneut herunterladen. Damit soll dem Recht auf Sicherungskopien genüge getan sein -- praktischerweise ohne dass man lokale Kopien zulassen muß. Datenherren, die so wagemutig sind, ihren Kunden zu erlauben, Kopien zu machen, auf andere Geräte zu übertragen oder auf

die PC-Daten einer kopiergeschützten Audio-CD zuzugreifen, können dies über den *Rights Locker* tun. Die Kunden müssen sich dafür jedesmal an das *Central Repository* wenden, das die Copyrights, die hier pikanterweise „*User Rights*“ heißen, freischaltet oder nicht -- ganz nach dem Geschäftsmodell des Rechteinhabers. Als „instantane Gratifikation“ bezeichnet es DWS, dass der Käufer einer *Secure CD* zum Anhören nur den Schlüssel herunterladen muß, nicht aber den Inhalt selbst.

Es ist noch gar nicht so lange her, dass wir uns daran gewöhnt haben, uns gegenüber Host-Rechnern zu identifizieren (Anfang der 1980er). Mit DRM müssen wir uns auch jeder einzelnen gekapselten Information gegenüber ausweisen. Die Zeiten, in denen wir ohne Identifikationszwang ein Buch lesen oder ein Album hören konnten, gehen dem Ende entgegen.

Wäre anonym nutzbares DRM denkbar? Prinzipiell ja (vgl. David Chaums eCash), aber niemand in der Branche arbeitet daran. DRM-Systeme dienen ja gerade dazu, zu kontrollieren, wer was wann wie und wo nutzt. Deshalb ist Anonymität ein Feature, das ohne gesetzliche Auflagen nicht eingebaut werden wird.

### ***Nutzungsvokabular: wann, wo auf welche Weise?***

Nutzungsvokabulare, im Branchenjargon *Rights Expression Languages* (REL), sind das Herzstück von DRM -- die Bausteine, aus denen Geschäftsmodell montiert werden.

Willems Buhse von DWS berichtete auf der Konferenz „Digital Rights Management 2002“, er und seine Kollegen hätten auf eine Musik-CD geschaut und dort 60 einzelne „Rechte“ entdeckt. Gemeint sind nicht etwa 60 Objekte oder Rechteinhaber, sondern Nutzungsformen wie Darstellen (auf Monitor oder Lautsprecher), beschränkte Anzahl oder Zeit von Darstellung, Drucken, Extrahieren (cut-and-paste), auf CD Brennen, Erstellen einer Sicherheitskopie, einer analogen Kopie, Verleihen, Weiterverkaufen etc. (Buhse 2002)

Ein prominentes Beispiel ist die *eXtensible rights Markup Language* (XrML). Sie geht auf Entwicklungen von Mark Stefik am Xerox PARC zurück und wird von ContentGuard, einem Joint Venture von Xerox und Microsoft vermarktet. Die Weiterentwicklung ist an OASIS übergegangen, das Konsortium zur Entwicklung von XML insgesamt und an die MPEG-Gruppe in ISO. XrML erlaubt es festzulegen, wer eine digitale Ressource (Content, Dienstleistung oder Software) nutzen darf, welche Nutzungen er oder sie vornehmen darf und unter welchen Bedingungen.

### ***Widerrufung und Systemerneuerung***

Da sich die Hoffnung auf ein statische ein-für-allemal sicheres System als Denkfehler erwiesen hat, enthalten alle aktuellen DRM-Systeme Mechanismen zur Fernwartung und Erneuerung. Verbreitet sich wieder einmal ein Hack des Windows Media Players, spielt Microsoft in sämtlichen installierten Playern einen *Patch* ein, der ihn unwirksam macht. Den Nutzern hat das Unternehmen bei der Installation per Lizenz die Einwilligung abverlangt, dass Microsoft den Player und DRM-relevante Komponenten des Betriebssystems jederzeit ungefragt über das Netz updaten darf (Foster 2/02, Sieling 7/02).

Kompromittierte Geräte, Programme oder Daten, deren DRM-System nicht auf diese Weise erneuert werden kann, werden mit Hilfe der *Device Revocation* ausgeschaltet. Diese berüchtigte Erfindung der *Digital Transmission Licensing Administration* beruht auf einer schwarzen Liste von Geräten, für die Umgehungen bekannt sind. Beim Authentifizierungsdialog zwischen Content und Abspielumgebung wird diese Liste ausgewertet. Trifft ein „legitimiertes“ Gerät dabei auf eines, dessen ID in der aktuellen Wiederrufungsliste steht, bricht es die

Verbindung ab. Auf diese Weise können die Datenherren einzelnen oder ganzen Klassen von Geräten und Programmen per Fernbedienung die Existenzberechtigung entziehen.

### **Suchmaschinen und Filterung**

Für den Fall, dass alle anderen Abwehrmechanismen versagen, dienen spezielle Suchmaschinen dazu, die entkommenen Objekte anhand von Wasserzeichen oder anderen Merkmalen im Netz ausfindig zu machen. Der Rechteinhaber kann dann den Anbieter oder seinen Provider unter Androhung von Rechtsmitteln auffordern, die Datei zu entfernen.

Befindet sich der Anbieter außerhalb der Wirksamkeit eines solchen *Notice-and-Takedown*, könnten Netzfilter zum Einsatz kommen. Die nichtautorisierten Dateien lägen immer noch im Netz, aber die betroffenen Nutzer könnten nicht mehr darauf zugreifen. Der Düsseldorfer Regierungspräsident Jürgen Büssow, der verfügt hat, dass die nordrhein-westfälischen Provider einen solchen URL-Filter einrichten sollen, legitimiert dies publikumswirksam mit der Sperrung von Nazi-propaganda und Kinderpornographie. Doch einmal installiert, ist abzusehen, dass auch die Datenherren ihre Ansprüche anmelden werden, mit dem System gegen Urheberrechtsverstöße vorzugehen.

### **Integrierte Systeme**

Bei aktuellen Systemen werden die Einzeltechnologien wie Content- und Transaktionsverschlüsselung, Wasserzeichen und Fingerabdrücke, Scrambling und Widerrufung zu gestaffelten „Verteidigungslinien“ kombiniert. Philips und Sony haben ihre neue *Super Audio CD* mit fünf „*lines of defense*“ ausgestattet. Auf heutigen DVDs befinden sich bis zu 10 verschiedene Systeme.

DRM-Diensteanbieter wie IBM (EMMS) und Bertelsmann (DWS) stellen eigene DRM-Technologien und die Dritter wie Microsoft und Adobe mit generischen eCommerce-Elementen wie Kundenverwaltung und Abrechnung zu End-to-End Systemen zusammen. Ein Verlag bekommt hier alles aus einer Hand, von der Werkproduktion über Packaging, Rechte- und Finanz-Clearing bis zur Auslieferung und Nutzungskontrolle in Endgeräten wie PC, PDA und Mobiltelefon.

### **Zentrale Instanzen**

Ein entscheidender Baustein dieser Infrastruktur ist eine zentrale Zertifizierungsinstanz, die die Einhaltung der DRM-Standards sichern, die Zertifikate kompromittierter Geräte widerrufen und als Schlichtungsstelle dienen soll. Stefik nannte sie *Digital Property Trust* (DPT). Aus der Logik des Systems heraus ist sie unerlässlich, setzt aber voraus, dass Content-, Geräte- und Informatik-Industrie sich darauf einigen könnten. Die streiten sich jedoch vor allem in verschiedenen Industriekonsortien und öffentlichen Standardisierungsgremien darum, wie technische Rechekontrolle überhaupt funktionieren soll und wessen patentierte Technologie zum verbindlichen Standard erhoben wird.

Die Standardisierung von Technologien erfolgt entweder in öffentlichen Gremien wie der ISO, IEEE, der MPEG oder JPEG, in Industriekonsortien wie dem W3C oder der SDMI, oder schließlich durch einzelne Unternehmen die qua Marktmacht einen de-facto Standard durchsetzen können. Auf die Rolle von Microsoft wird gleich noch näher einzugehen sein, ebenso auf die TCPA. Hier einige wichtige Beispiele für Konsortien:

In der SDMI sitzen über 180 Unternehmen der Musik-, Geräte- und

eCommerce-Industrie.

1998 bildete sich die *Copy Protection Technical Working Group* (CPTWG). Heute sitzen dort Vertreter der Branchen Geräte (Panasonic, Thomson, Philips), Content (Warner Bros., Sony Pictures, MPAA), DRM (Macrovision, Secure Media), Telekom (Viacom, Echostar Communications) und Informatik (Intel, IBM, Microsoft) zusammen.

In der *DVD Copy Control Association* (CCA) hat die Filmindustrie eine nichtgenannte Zahl von Technologieunternehmen um sich geschart, um CSS, Regionenkontrolle und Wasserzeichen zu entwickeln. Ihr ging 1995 das DVD Consortium voraus, das heute DVD Forum heißt und etwa 230 Mitglieder hat. Wenn so viele zusammensitzen, kann es nur Streit geben. So scheiden sich z.B. bei der wiederbeschreibbaren DVD die Geister. Das DVD Forum verfolgt die DVD-RW, während die DVD+RW Alliance um Dell und HP ihr System DVD+RW nennt (man beachte den feinen typographischen Unterschied).

Die Breite der strategischen Allianzen macht deutlich: hier geht es nicht um eine Einzeltechnologie, wie einen neuen Dongle, nicht darum, Schlösser nur an Musikdateien und Videostreams anzubringen. Es geht um eine systemweite Grunderneuerung, bei der kein digitaler Stein auf dem anderen bleiben wird.

### **Bündelverträge**

Die Vertragsfreiheit der Datenherren besteht darin, ihre Inhalte in einer bestimmten DRM-Architektur anzubieten oder eben nicht. Die Hardware-Hersteller in der Konsumelektronik- und der Informatikindustrie dagegen haben keine Wahl. Ein Hersteller von DVD-Playern z.B. muß CSS lizenzieren, da Hollywood seine Inhalte nur auf CSS-verschlüsselten Scheiben anbietet, ein Geräte ohne CSS also unverkäuflich wäre. Das lizenziert ihm aber die DVD Copy Control Association, Inc. (DVD CCA) nur, wenn er auch andere DRM-Komponenten wie Kopierschutzverfahren von Macrovision, Regionenmanagement, CGMS, DTCP und HTCP in seine Geräte einbaut. Stefan Bechtold zufolge ist dies ein allgemeines Charakteristikum von DRM-Technolizenzverträgen, das damit begründet wird, dass nur durch die vertragliche Kopplung unterschiedlicher DRM-Komponenten auf dem Endgerätemarkt ein "einheitliches und durchgängiges Schutzniveau" geschaffen werden könne. Dass eine solche Politik der gekoppelten Technolizenzen kartellrechtliche Frage aufwirft, scheint offensichtlich, doch werden sie erstaunlicherweise bislang weder von gesetzlichen Vorschriften noch auch nur in der juristischen Literatur behandelt, so Bechtold (Bechtold 2002: 178 ff.)

### **Beispiel: Microsofts Windows Media Rights Manager**

Kernstück von Microsofts heutiger DRM-Architektur ist der *Windows Media Rights Manager*, in der ersten Version im August 1999 vorgelegt. Er ist Bestandteil von *Microsoft Windows Media*, sowohl auf der Seite der Produzenten (Media Tools für die Content-Aufbereitung, die *Windows Media Format Software Development Kits* (SDKs)), der Distributoren (Media Services, Streaming-Technologie für Audio und Video, Digital Asset Server), wie der Rezipienten (Windows Media Player, eBook Reader). Er ist ebenfalls integriert in die aktuellen Microsoft-Betriebssysteme Windows ME und XP, sowie die verteilte Objektarchitektur .NET.

Nach Angaben von Microsoft gibt es derzeit mehr als 450 Millionen installierte Media Player. Demnach hätte fast die gesamte geschätzte Weltbevölkerung des Internet (NUA Internet Surveys) einen MS Audio- und Video-Player mit einem MS DRM. Das ist nicht verwunderlich, wird er doch zusammen mit allen aktuellen MS-Betriebssystemen und somit auf 95% aller PCs vorinstalliert ausgeliefert.

Darüberhinaus ist er verfügbar für alle gängigen Windows-Varianten, Mac OS einschließlich X, Pocket PC, Solaris und verschiedene Handhelds und Palms. Ebenso wenig verwunderlich ist es daher, dass die meisten Content-Anbieter ihre Waren ausschließlich oder auch im Windows Media-Format bereitstellen. Im Streaming-Markt hat Microsoft nur noch Konkurrenz von Real Networks und Apples Quicktime. Letzteres implementiert zwar als erstes den neuen ISO-Standard MPEG-4, dem Nachfolger von MP3 Audio und MPEG-2 Video, doch ob der de-jure Standard sich gegen den de-facto Standard durchsetzen kann, muß sich erst zeigen.

Der Rights Manager verschließt jede Mediendatei mit einem Lizenzschlüssel, der beim Download auf einen bestimmten Rechner hin geprägt wird. Auch der Player selbst wird beim Download auf die Hardware-ID des jeweiligen Rechners hin "individualisiert". Kompromittierte Player können so nicht weiterverbreitet und während der Content-Lizenzierung ausgeschaltet werden ("Revocation"). Die gesamte Medien-Bibliothek ist somit an einen einzigen Rechner gekoppelt. Mit dem "Personal License Migration Service" kann der Kunde dann Mediendateien durch eine Online-Neulizenzierung auf dem jeweiligen Zielrechner auf bis zu zehn Rechner übertragen und mit dem *Windows Media Device Manager* auch auf SDMI-konforme portable Geräte.

In Version 7 des Windows Rights Managers umfassen die verkaufbaren Nutzungsrechte ("*Business Rules*"): Verfallsdatum, unbeschränkte Darstellung, Übertragung auf ein SDMI-konformes Gerät, auf CD Brennen, Beginn und Ende einer Nutzung, Dauer, Anzahl der Darstellungen oder Transfers.

Content und Lizenz werden getrennt verbreitet. Versucht man, ohne Lizenz eine Medien-Datei abzuspielen, wird man auf eine Webseite geleitet, auf der man eine Lizenz erwerben kann ("virales Marketing"). Außerdem können auf diese Weise die Lizenzbedingungen auf dem Server einfach geändert werden, ohne dass der Content widerrufen und neu verbreitet werden müßte.

Da Microsoft festgestellt hat, dass viele Nutzer von umständlichen Authentifikations- und Lizenzierungsdialogen entnervt sind, hat es sich eine "transparente" (will sagen: für den Nutzer unsichtbare) "stille Lizenzierung" ausgedacht: "Silent licensing means that a content provider may deliver the license to the consumer without the need for the consumer to type more information." (Microsoft, DRM Features)

Eine strukturelle Schwäche aller DRM-Systeme ist, dass der Content bei aller Sicherung letztendlich dargestellt, dazu entschlüsselt und dekodiert werden muß und in dem Moment abgefangen werden kann. Dagegen geht Microsoft auf Betriebssystemebene vor. Windows ME und XP legen einen *Secure Audio Path* zwischen Player und Sound-Karte. Doch das ist erst der Anfang.

### **3. Secure Boot**

Nach der Entwicklung von lokalen zu vernetzten Lösungen, beginnt nun die globale Neustrukturierung des Cyberspace. Im militärischen Bereich denkt man seit spätestens Anfang der 1970er darüber nach, wie man durch einen kontrollierten Boot-Vorgang einen gewöhnlichen Computer in einen gesicherten Zustand versetzen kann. Die ersten Modelle für einen sicheren Boot sahen kryptographische Koprozessoren vor. Das wurde verworfen, weil es architektonische Veränderungen in den meisten Computersystemen voraussetzt, und das würde einen ungeheueren industrie-übergreifenden Koordinationsaufwand erfordern. Oder ein Monopol, wie wir gleich sehen werden.

Eine der ersten sicheren Bootstrap-Architekturen stellten David Farber und zwei

Kollegen von der University of Pennsylvania 1996 unter dem Namen AEGIS vor. Ausgehend von einem vertrauenswürdigen BIOS-Segment in einem zusätzlichen PROM werden nacheinander das zweite BIOS-Segment, die Hardwarekarten, der Boot-Block, das Betriebssystem und schließlich die Anwendungsprogramme überprüft und gestartet. Zur Überprüfung wird ein kryptographischer Hash der Komponente errechnet und anhand einer gespeicherten Signatur verifiziert. Scheitert die Prüfung, sehen sie einen Recovery-Mechanismus über IPv6 von einem vertrauenswürdigen Netzrechner vor. Sie stellten ihre Arbeit in den Kontext des explosiv wachsenden E-Commerce, aber es ging ihnen nicht um DRM, sondern generell um Zugangskontrolle, die auch Schutz vor Viren, Trojanern usw. bietet. Ihr Modell hat ein als vertrauenswürdiger verifiziertes System zum Ergebnis. (Arbaugh, Farber, Smith 1996)

### **TCPA**

Im Oktober 1999 gründeten Intel, Compaq, HP, IBM und Microsoft die *Trusted Computing Platform Alliance* (TCPA), der sich mehr als 180 weitere Unternehmen angeschlossen haben. Im Board of Advisors treffen wir David Farber wieder. Ihr Ziel ist es, die Sicherheit auf der Ebene von Plattform-Hardware, BIOS, System-Software und Betriebssystem zu verbessern. „The objective of the TCPA is to make trust just as much a part of the PC platform as memory and graphics.“ (TCPA, Januar 2000)

Kernstück der TCPA-Technologie ist daher ein kryptographischer Koprozessor namens „*Trusted Platform Module*“ (TPM). Er verfügt über einen Zufallsgenerator, nichtflüchtigen Speicher für Schlüssel und Mechanismen für die Generierung und Verwaltung von Schlüsseln, Signaturen und von Hashes.

Auf dieser physikalischen Kryptoinfrastruktur setzt der *TCPA Software Stack* (TSS) auf. Er verwendet „Integritätsmetriken“ zur Authentifizierung des Systems. Die Erzeugung von kryptographischen Zusammenfassungen der Komponenten wird als „Selbstinspektion“ bezeichnet.

Das TPM übernimmt den Systemstart und authentifiziert als erstes den BIOS Boot Block. Das BIOS fragt dann, z.B. über eine SmartCard oder eine Biometrieprüfung ab, ob ein autorisierter Nutzer am Rechner sitzt. Es folgt die Authentifizierung des Programms, das das Betriebssystem lädt, das wiederum den Betriebssystemkern überprüft. Wenn alle Überprüfungen erfolgreich, ist gewährleistet, dass sich keine unerwünschten Programme eingeschlichen haben und der Kernel das System vollständig kontrolliert. Schließlich startet das Betriebssystem auf dieselbe Weise die Anwendungsprogramme.

Die Ergebnisse der „Integritätsmessungen“ des TSS werden im TPM abgelegt. Will nun ein Content-Anbieter entscheiden, ob er diesem System seine kostbaren Waren anvertrauen möchte, schickt es ihm die signierten kryptographischen Zusammenfassungen der aktuellen Konfiguration. Das TCPA-System attestiert also nur einen gegebenen Systemzustand und überläßt es dem Gegenüber, dessen Vertrauenswürdigkeit zu bewerten. Dringt nun ein Virus in dieses System ein, verändert es den gemessenen Systemzustand und der Zugang zu Daten kann gesperrt werden. Das Gegenüber kann auch ein lokaler Medien-Player sein, der den kostbaren Inhalte aus dem lokalen gesicherten Speicher nur freigibt, wenn nicht gleichzeitig ein vertrauensunwürdiges Programm geladen ist.

Das System schaltet keine Software ab oder blockiert Daten, sondern präsentiert einem Transaktionspartner gleichsam ein Röntgenbild des aktuellen Systemzustands.

Die erste TCPA-Spezifikation wurde im Januar 2001 veröffentlicht. National

Semiconductor und Infineon produzieren die Koprozessoren. IBM bietet seit April TCPA-konforme Laptops an, und Windows XP und auch Microsofts X-Box enthalten TCPA-Features.

Dem Konsortium geht es ums Ganze. Um die Plattform PC sicherer zu machen, sei eine flächendeckende Lösung erforderlich. „The concept of ubiquity ... implies that at some point, all PCs will have the ability to be trusted to some minimum level. ... Every PC will have hardware-based trust, and every piece of software on the system will be able to use it.“ (TCPA, Januar 2000). Dazu will das Konsortium einen Industriestandard etablieren, doch bislang hat sich trotz endloser Presserklärungen außer den Mitgliedern niemand wirklich dafür interessiert. Und mindestens eines der Mitglieder zieht es vor, eigene Standards zu setzen.

#### **4. Krypto-Infrastruktur (Palladium)**

Im Dezember 2001 meldete Microsoft ein DRM-Betriebssystem zum Patent an, das die meisten der genannten Elemente eines *Secure Boots* enthält. Ein Patent ist noch kein Produkt. Und in diesem Fall ist es noch nicht einmal ein sicheres Patent. Microsofts Anmeldung wird von DRM-Pionier InterTrust angefochten, das darin seine eigene geschützte Technologie wiedererkennt. Ein erstes Betriebssystemprodukt, das einige der im Patent beschriebenen Mechanismen verwendet, kündigte Microsoft im Juli diesen Jahres an. Edelfeder Steven Levy erhielt die Rolle des Newsbreakers (Newsweek, 1. July, vorab auf MSNBC). Er sparte nicht mit Superlativen: „Microsoft’s plan to literally change the architecture of PCs ... one of the riskiest ventures the company has ever attempted,“ so Levy. „It’s one of the most technically complex things ever attempted on the PC,“ so ein Gartner-Analyst.

Über die Funktionen von Palladium erfahren wir von Levy wenig. Er zählt eine Reihe möglicher Anwendungen auf, darunter generische Sicherheits- und Datenschutzaspekte. Es stoppe Viren und Würmer, beseitige Spam, und werde Filmstudios und Platten-Labels angeboten werde, um ihre Waren per DRM zu verkaufen. Und auch das ist nur zum Nutzen der Nutzer, denn es könne ihnen erlauben, „to exercise ‚fair use‘ (like making personal copies of a CD)“. Ein pikantes Feature erfahren wird noch: „the system’s ability to ineluctably log [employees’] e-mail, Web browsing and even instant messages.“ Levy schiebt den genüßlichen Kommentar von Windows-Zar Jim Allchin nach: „I have a hard time imagining that businesses wouldn’t want this.“ (Levy 2002)

Die Hardware-Neuerungen von Palladium bestehen aus einem kryptographischen Koprozessor und strukturellen Änderungen in der CPU, im Chip-Satz und in Peripheriegeräten wie Tastatur und Drucker. Herzstück ist die *Security Support Component* (SSC), ein Prozessor mit einem kleinen nicht-flüchtigen Speicher, ähnliche einer Smart-Card. Genauso wie das TPM der TCPA kann die SSC kryptographische Operationen ausführen und Schlüssel speichern, nur das hier für die symmetrische Verschlüsselung AES statt 3DES vorgesehen ist. Ebenso nützen hier die maschinenspezifischen Schlüssel, wenn sie einem Hardware-Angriff zum Opfer fallen, nur etwas auf dem betroffenen System, das sich zudem als kompromittiert zu erkennen gibt und daher von gesicherten Diensten ausgeschlossen werden kann (*revocation*).

Wer diese Hardware-Komponente herstellen wird, ist noch nicht bekannt. Die neuen CPUs kommen von AMD und Intel. „A whole new class of processors not differentiated by speed, but security,“ zitierte Levy einen AMD-Vertreter. Intel hat angekündigt, dass „LaGrande“, der Nachfolger des Pentium 4 in der zweiten Hälfte 2003 Palladium unterstützen wird. AMD sagt, sie hätten die Chips, wenn der Markt

danach verlangt. Bei der Hardware-gesicherten Verbindungen zu Tastatur und Bildschirm, die das Abfangen und Einspielen von Signalen verhindern soll, handelt es sich offenbar um eine Erweiterung des *Secure Audio Path*, der die Strecke zwischen CPU und Sound-Karte verschlüsselt.

Im Zentrum der Software-Elemente von Palladium steht der „Nexus“. Er entspricht dem *TCPA Software Stack*. Mit Hilfe der Dienste der SSC erzeugt er eine gesicherte Betriebsumgebung namens *Trusted Space*. Nexus authentifiziert Hard- und Software und kann den signierten Systemzustand gegenüber einer Online-Bank oder einem Content-Anbieter attestieren. Palladium-Anwendungen („*trusted agents*“) führt er in jeweils eigenen gesicherten Bereichen des *Trusted Space* aus, die physikalisch und kryptographisch isoliert sind. Jeder dieser getrennten „Tresorräume“ (*vaults*) ist mit seinen eigenen Schlüsseln und *policies* ausgestattet, die die Kommunikation von und zu den Agenten regeln und die vom Nutzer, der IT-Abteilung eines Unternehmens, einem Online-Händler oder -Diensteanbieter festgelegt werden. Die dazugehörigen Daten werden ausschließlich verschlüsselt auf der Festplatte gespeichert und können an die Maschine, den Nexus oder die Anwendung gekoppelt werden.

Palladium wird als eine Ausführungsumgebung parallel zum herkömmlichen Windows Betriebssystem präsentiert, ein auf einer eigenen Hardware aufsitzen, getrennter Software-Stack mit Nexus als einer Art Mikrokern, der nicht auf den ungesicherten Bereich durchgreift. „Since Palladium does not interfere with the operation of any program running in the regular Windows environment, everything, including the native OS and viruses, runs there as it does today. ... realms allow a user to have a locked-down work environment and fully open surfing environment at the same time, on the same computer.“ (White Paper)

Es handelt sich also offenbar um eine „Sandkasten“-Architektur, wie sie Sun mit seiner *Java Virtual Machine* eingeführt hat. Potentiell bösartige Java-Applets, denen man im Web begegnet, werden dabei in einem von der übrigen Laufumgebung abgeschirmten Speicherbereich ausgeführt -- gewissermaßen in einem Rechner im Rechner. Java-Applets haben standardmäßig keine Lese- und Schreibrechte und nur beschränkte Zugriffsrechte auf das Umgebungsbetriebssystem. Bei Palladium dient der Sandkasten dem inversen Zweck: nicht die Laufumgebung soll vor seinem Inhalt gesichert werden, sondern dieser gegen Zugriffe von dort. Darin scheint auch der Hauptunterschied zum TCPA-Modell zu liegen: Die TCPA-Technologie überwacht den Bootvorgang und den Zustand des gesamten Systems, während Palladium sich auf die Sandkiste beschränkt.

Vertrauenswürdig für wen? Das ist die Frage, die sich jedem stellt, der sich mit *trusted systems* beschäftigt. Microsoft stellt in den Internet-öffentlichen Papieren durchgängig die Vorteile und den Datenschutz für individuelle Nutzer heraus. Die Vorteile für Content-Provider werden, wenn überhaupt als letztes genannt. Die Kontrolle über seine persönlichen Daten und die Funktionen des Systems läge ganz allein beim Nutzer. Die Palladium-Funktionen sollen wie bei der TCPA standardmäßig ausgeschaltet und per Schalter deaktivierbar sein. Es entsteht eine Situation wie bei Cookies: Man kann sie deaktivieren, ist dann aber von bestimmten Diensten ausgeschlossen.

Wie die TCPA sieht Microsoft voraus, dass der maschinenspezifische öffentliche Schlüssel nicht direkt, sondern in der Regel nur zur Zertifizierung von Zufallsschlüsseln durch einen „*pseudo-identity provider*“ des eigenen Vertrauens verwendet wird (MS FAQ). Steht uns also dank Microsoft eine Zeit des pseudonymen Surfens bevor? Das White Paper macht dazu zwei Aussagen:

„Palladium authenticates software and hardware, not users“ und „A closed sphere of trust binds data or a service to both a set of users (logon) and to a set of acceptable applications.“ Dass für die Kommunikation mit Bank und Content-Provider eine personenbezogene Identifikation erforderlich ist, versteht sich. Auch die erste Aussage ist korrekt, verschleiert aber die Tatsache, das Palladium, um Daten an Nutzer binden zu können, die Dienste von Chip-Karte, Biometrie-Modul, Passport oder ähnlichem verwenden wird. Palladium ist somit vielmehr ein Schlüsselbaustein in einer Welt des allgegenwärtigen Identifikationszwangs.

Eine „feinmaschige Zugangskontrolle“ soll dem Anwender erlauben zu bestimmen, welche Rechte Programme bekommen und wie und wem Personendaten preisgegeben werden (MS FAQ). Diese Aussage steht allerdings im Widerspruch zum neuen Design-Ziel, das Microsoft für seine Windows Media Suite verkündet hat. Da Zertifikatsannahmedialoge und ähnliche Prozeduren die „*User Experience*“ stören, solle DRM „transparent“, also unsichtbar für den Nutzer funktionieren („*silent licensing*“). Aus demselben Grund ist kaum damit zu rechnen, dass Palladium seine Nutzerin tatsächlich bei jeder Operation um Erlaubnis fragt.

Neben Datenschutzfragen gibt sich Microsoft große Mühe, den -- gegenüber einem Monopol erwartbaren -- kartellrechtlichen Bedenken zu begegnen. Palladium wie TCPA funktionieren nur, wenn sie ubiquitär verbreitet sind. Wer „buchstäblich die Architektur des PC verändern“ will, braucht dazu Partner. Daher will Microsoft sein System als eine „kooperative Konsumenten- und Industrieinitiative“ entwickeln und das Feedback von Daten- und Konsumentenschützern, Sicherheitsexperten, Staat und sämtlichen anderen Parteien berücksichtigen. „The Palladium technology must be broadly adopted to be fully effective ... it's something that everyone across the landscape of computing needs to be invested in.“ (Manferdelli)

Alles soll offen sein. Microsoft will Drittanbieter von alternativen Nexusen zulassen. Neben Microsoft sollen auch andere Palladium-Hard- und Software zertifizieren dürfen. Niemand soll ausgeschlossen werden. Freie Betriebssysteme wie GNU/Linux und FreeBSD sollen weiterhin auf der Palladium-Hardware laufen. Technisch sei es möglich, auch einen Nexus für diese Plattformen zu entwickeln, allerdings müssten Fragen des geistigen Eigentums geklärt werden, da das Palladium-Design patentiert ist (MS FAQ). Das Unternehmen grenzt sich ab gegen andere „übermäßig restriktive“, nutzerunfreundliche, geschlossene DRM-Systeme. „Unlike closed, captive platforms, ‚Palladium‘ allows any provider or even individual to build a trustworthy interoperable mechanism that is not in the exclusive control of a single entity.“ Für ein Unternehmen, dessen Strategien zur Zementierung seiner *captive platform* gerichtsnotorisch sind, eine erstaunliche Aussage.

Microsoft hat sogar angekündigt, dass es den Quellcode des Nexus im Rahmen der *Shared Source Initiative* veröffentlichen wird. Eine breite Überprüfung solle die Sicherheit der Software gewährleisten. „The beauty of publishing the nexus source code is that this is a type of technology that even when known, still can't be broken. In fact, knowing what's going on is going to be essential to being able to trust it.“ (Manferdelli) Auch das ist eine erstaunliche Kehrtwende, setzt das Unternehmen doch gleichzeitig seine FUD-Kampagne gegen den Einsatz freier Software besonders durch die öffentliche Hand fort, da sie durch ihre Quelloffenheit inhärent unsicher sei.

Microsofts Einladung zur allseitigen Kooperation verliert durch seine Haltung gegenüber der TCPA erheblich an Glaubwürdigkeit. Laut FAQ ist Palladium ausdrücklich keine Implementierung der Spezifikationen der *Trusted Computing Platform Alliance*, also des von ihm selbst mitgegründeten Konsortiums mit genau dem Ziel, einen ubiquitären Industriestandard zu entwickeln. TCPA und Palladium

hätten gemeinsame Merkmale wie Attestierung und versiegelten Speicher, aber eine „grundlegend verschiedene Architektur.“

Nach Unterschieden muß man in der teilweise wortgleichen Argumentationen allerdings suchen. Was bleibt, ist der Hochsicherheits-Sandkasten als struktureller Unterschied zur TCPA-Technologie, die beim Booten die gesamte Plattform authentifiziert. Doch wenn dies eine Verbesserung gegenüber der gemeinsam entwickelten Architektur ist, warum hat Microsoft sie nicht in das Konsortium eingebracht? Der Hauptunterschied zwischen *Trusted Computing* und *Trustworthy Computing* scheint darin zu liegen, wessen Patente zum Zug kommen und wer den Ton angibt.

Auffällig ist die Vehemenz, mit der Microsoft Palladium von DRM abgrenzt. Die beiden hätten überhaupt nichts miteinander zu tun. Palladium stelle wiederum nur Funktionen bereit, die von DRM-Systemen verwendet werden können. Damit geht eine Neudefinition von DRM einher, über die ich eingangs gesprochen hatte.

Unter den Microsoft-Kremelogen hält sich die Einschätzung, dass Palladium in der nächsten Windows-Version enthalten sein wird, die unter dem Codenamen „Longhorn“ für 2004 angekündigt ist.

## Fluchtpunkt Abschaffung des Universalmediums

*Conventionally, we use general-purpose computers with general-purpose operating systems and general-purpose programs. The computer industry, grounded on the premise that computers can do anything that can be programmed in software, produces a wide range of programs [...], and both hardware and software are intended for general purposes -- that is, any purpose the user wants to put them to. [...] Stuck within this framework, the community of computer users protests against any attempt to regulate the copying of digital property. [...] Honoring their [writers of words, interactive games, and songs] creative works in the digital systems of tomorrow requires us to challenge the design assumptions of the systems we use today. (Stefik, 1996, S. 10 f.)*

Mike Godwin beschreibt in seinem Aufsatz "Hollywood Versus the Internet" einen Clash of Cultures zwischen den Industrien der Alten Medien, die ihre Kunden als „Konsumenten“ ansehen und den Informatikindustrien, die ihre als Anwender oder Nutzer sehen. Hier werden *Couchpotatoes* mit Medienkonserven gefüttert, dort trägt man zum *Empowerment*, einer Befähigung und Aktivierung der Nutzer bei:

*„Building DRM into all of this [die Architektur des PCs] -- limiting how computers perform their basic functions -- seems to the Tech Faction almost to be an effort to make a computer something other than a computer -- a digital appliance, maybe, or something special-purpose like a toaster. It's an approach that would have the effect of undoing the user-empowerment philosophy that drove the PC revolution in the first place.“ (Godwin 2001)*

So absurd es erscheinen mag, genau darauf zielt in logischer Konsequenz die Konterrevolution des DRM-Projekts. Der US-amerikanische Kryptographieexperte Bruce Schneier schrieb: "If you think about it, the content industry does not want people to have computers; they're too powerful, too flexible,

and too extensible. They want people to have Internet Entertainment Platforms: televisions, VCRs, game consoles, etc.” (nach Godwin 2001)

Wenn ein umfassendes DRM-Szenario Wirklichkeit wird, was bleibt dann vom frei programmierbaren Universalmedium? Wenn neue Hardware und “*secure boot*” tatsächlich das Starten eines alternativen Betriebssystems unterbinden, nichts. Doch selbst wenn die Hardware dies zuließe, ist der PC ab dem “*secure boot*”, also dem Zeitpunkt, wo er für alle praktischen Belange zu einem frei programmierbaren Allzweckrechner wird, dank der Datenherrentechologie bald genau kein solcher mehr. Ein “modifizierter Universalrechner”, wie es in Microsofts DRM-Betriebssystempatent heißt, ist keiner, denn eine Maschine kann genausowenig ein bißchen universal sein, wie frau ein bißchen schwanger sein kann.

Mit Microsofts Sandkasten-Architektur entsteht im günstigsten Fall eine Zweiklassengesellschaft im Computer: die Palladium-gesicherten Bereiche mit ihren Privilegien, wie dem Zugang zu kommerziellen Multimediatechnologien, und der Rest, in dem weiterhin „böartige“ Software wütet und in dem der Nutzer ohne Sicherheitsausweis Programme starten und programmieren darf.

Im schlimmsten Falle steht uns also eine Spaltung in Computer als Produktions- und andere als Konsumtionsmittel bevor, ähnlich wie bei der DAT-Technologie, wo in Konsumentengeräten ein *Serial Copy Management System* gesetzlich vorgeschrieben, aber die teuren “professionellen” Studiogeräte frei davon sind. Dann muß natürlich der Zugang zu diesen „freien“ Rechnern kontrolliert werden. Nach Stallmans Szenario könnten nur noch professionelle, mit einer Art Amateurfunklizenz oder Waffenschein zertifizierte Programmierer und Systemadministratoren legal von der Allzweckmaschine Gebrauch machen. Für den Rest von uns gäbe es nur noch reine Medienabspielgeräte. Hier das Programmierwerkzeug, dort “vending machines” -- *and never the twain shall meet*. Das wäre das traurige Ende der Konvergenz.

Die Technik verfolgt das Ziel, aus der *Universal Machine* eine *Conditional Access Machine* zu machen. Und die Zugangsbedingungen werden von Anbietern bestimmt und per Fernbedienung festgelegt, überwacht, aktualisiert und widerrufen. Eine Welt am Draht steht uns bevor. An die Stelle des *User-Empowerment* durch die Revolution von PC und Internet bekämen wir das *Disempowerment* durch die DRM-Konterrevolution. Bruce Schneier schrieb in einer ersten Einschätzung von Microsofts jüngstem Coup:

*„My fear is that Palladium will lead us down a road where our computers are no longer our computers, but are instead owned by a variety of factions and companies all looking for a piece of our wallet.“* (Schneier 8/02)

## Literatur

Levy, Steven, „The Big Secret. An exclusive first look at Microsoft’s ambitious-and risky-plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it?“, Newsweek, 1. Juli 2002, vorabveröffentlicht auf MSNBC: <http://www.msnbc.com/news/770511.asp?cp1=1>

Microsoft, Palladium White Paper: A Business Overview, August 2002,  
<http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp>

Microsoft Palladium Initiative Technical FAQ - August 21, 2002,  
<http://www.microsoft.com/technet/security/news/PallFAQ2.asp>

Microsoft, DRM Features,  
<http://www.microsoft.com/windows/windowsmedia/WM7/DRM/features.asp>

Stallman, Richard, Words to Avoid,  
<http://www.gnu.org/philosophy/words-to-avoid.html#DigitalRightsManagement>

Bechtold, Stefan, Vom Urheber- zum Informationsrecht. Implikationen des Digital Rights Management, C.H. Beck, München 2002

European Commission, Commission Staff Working Paper: Digital Rights. Background, Systems, Assessment, SEC(2002) 197, Brussels, 14.2.2002, nicht mehr online

Grassmuck, Volker, Freie Software zwischen Privat- und Gemeineigentum, Bundeszentrale für politische Bildung, Bonn 2002, <http://freie-software.bpb.de/>

Pfitzmann, Prof. Dr. Andreas (technischer Teil), Prof. Dr. Ulrich Sieber (strafrechtlicher Teil), Gutachten: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen, erstellt im Auftrag von DMMV und VPRT (Hrsg.), September 2002, <http://www.vprt.de/aktuelles/veroeffentlichungen.html>

Buhse, Willems, „Business models for digital goods - scenarios for the music industry“, gehalten auf: Digital Rights Management 2002 (<http://www.digital-rights-management.de>), org. Forschungsverbund Datensicherheit NRW, DIHK et al., Berlin, 29.-30.1.2002, [http://www.eurubits.de/drm/drm\\_2002/audio/buhse.mp3](http://www.eurubits.de/drm/drm_2002/audio/buhse.mp3)

Foster, Ed, „Check the fine print“, in: InfoWorld, 8.2.2002, <http://staging.infoworld.com/articles/op/xml/02/02/11/020211opfoster.xml>

Sieling, Lars, „Auf leisen Sohlen vom Betriebs- zum DRM-System“, in: Telepolis 3.7.02, <http://www.heise.de/tp/deutsch/special/copy/12838/1.html>

Arbaugh, William A., David J. Farber Jonathan M. Smith, A Secure and Reliable Bootstrap Architecture, December 2, 1996, <http://www.cis.upenn.edu/~waa/aegis.ps>

TCPA, Building a Foundation of Trust in the PC, January 2000  
[http://www.trustedcomputing.org/docs/TCPA\\_first\\_WP.pdf](http://www.trustedcomputing.org/docs/TCPA_first_WP.pdf)

TCPA Specification/TPM Q&A, Updated 18 July, 2002,  
[http://www.trustedcomputing.org/docs/TPM\\_QA\\_071802.pdf](http://www.trustedcomputing.org/docs/TPM_QA_071802.pdf)

Schneier, Bruce, „Palladium and the TCPA“, in Crypto-Gram 15. August 2002,  
<http://www.counterpane.com/crypto-gram-0208.html#1>

Godwin, Mike, „Coming Soon: Hollywood Versus the Internet“, auf Cryptome.org, 18. Dezember 2001, <http://cryptome.org/mpaa-v-net-mg.htm>

Stefik, Mark J., „Letting Loose the Light: Igniting Commerce in Electronic Publication“, in: M. Stefik (Hrsg.), Internet Dreams: Archetypes, Myths, and Metaphors, MIT Press, Cambridge Mass. 1996 und <http://www.parc.xerox.com/istl/projects/uir/pubs/pdf/UIR-R-1996-10-Stefik-InternetCommerce-IgnitingDreams.pdf>