Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen

Eine Studie im Auftrag des Deutschen Multimediaverbandes (dmmv) e.V. und des Verbandes Privater Rundfunk & Telekommunikation (VPRT) e.V.

Technischer Teil

Verfasser:

Prof. Dr. Andreas Pfitzmann, Technische Universität Dresden
(Projektverantwortung)

Dr.-Ing. Hannes Federrath, Freie Universität Berlin
(Projektkoordination)

Dipl.-Inform. Markus Kuhn, University of Cambridge, England

13. März 2002

Kurzfassung

Inzwischen existiert eine Vielzahl von Techniken zum Schutz von Rechten an digitalen Inhalten. Diese sog. Digital-Rights-Management-Systeme (DRM-Systeme) sollen möglichst unabhängig von der Distributionsform (Datenträger, Rundfunkübertragung, Kommunikationsnetze etc.) und vom Typ (Multimedia-Inhalt, ausführbare Software, Publikation etc.) der zu schützenden Inhalte die Rechte der an der Produktion, Verteilung sowie dem Konsum digitaler Inhalte Beteiligten schützen helfen.

Die meisten verfügbaren Systeme bieten allerdings keinen oder nur sehr begrenzten Schutz gegen starke (clevere, intelligente) Angriffe. Inhalte, die über CD, DVD und das Internet verbreitet werden, sind heute technisch katastrophal schlecht vor Verfälschung und unberechtigter Vervielfältigung geschützt. Dies gilt auch für urheberrechtlich geschützte Inhalte. Die bekannten technischen Schutzmaßnahmen helfen bestenfalls gegen Gelegenheitstäter und auch das nur solange, bis (möglicherweise, aber nicht notwendigerweise illegale) automatisierte Verfahren zur illegalen Nutzung veröffentlicht werden.

Um die durch gesetzliche Vorschriften allein schwierig kontrollierbare unrechtmäßige Nutzung geistiger Werke einzudämmen, wurden eine Reihe von technischen Maßnahmen entwickelt. Man kann die Maßnahmen danach unterscheiden, ob sie bereits die illegale Nutzungsmöglichkeit verhindern sollen oder nur die illegale Nutzung. Ein Beispiel für ersteres wäre, bereits die Erstellung illegaler Kopien zu verhindern, ein Beispiel für letzteres, nur die Verwendung illegaler Kopien zu erschweren.

Bei den technischen Komponenten von DRM-Systemen handelt es sich im Wesentlichen um auf die speziellen Gegebenheiten von Multimedia-Daten-Kommunikation zugeschnittene IT-Sicherheitssysteme. Das bedeutet, die Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit – in konkreten Ausprägungen z.B. Nicht-Konsumierbarkeit nicht bezahlter Inhalte, Unverfälschbarkeit urheberrechtlich geschützter Werke, Verhindern von Piraterie/Anfertigen illegaler Kopien – werden durch kryptographische, organisatorische und spezielle Sicherheitsmechanismen unter einem bestimmten Angreifermodell realisiert.

Insbesondere Verfahren, die das Kopieren von Inhalten verhindern sollen, sind deutlich unsicherer gegenüber Verfahren, die auf die Einschränkung illegaler Nutzungsmöglichkeiten zielen und damit robuster gegen Angriffe. Da digitale Daten verlustfrei vervielfältigt werden können, wird meist versucht, das Speicher- bzw. Übertragungsmedium schwer kopierbar zu machen oder – nachdem die Daten gelesen wurden – diese niemals vor der Ausgabe (Bildschirm, Lautsprecher etc.) in hoher Qualität (digital) abgreifbar zu machen bzw. noch innerhalb des speziell geschützten Bereiches, der meist in Hardware realisiert ist, in eine nur mit Verlusten kopierbare Repräsentation (z.B. analoges Signal) zu bringen.

Einige Verfahren sind ausschließlich in Software realisiert und bieten – da die Ausführung der Software nicht vor der ausführenden Maschine geschützt werden kann – nur sehr rudimentären,

begrenzten Schutz. Alle Software-Maßnahmen schützen die Anbieter von Inhalten selbst kurzfristig nahezu nicht vor Piraterie. Sogar technisch ungebildete Laien können zu Piraten werden, sofern sie sich der im Internet oftmals kostenlos angebotenen Software-Werkzeuge bedienen, die nahezu als Abfallprodukt der notwendigen Erforschung von Sicherheitsmechanismen entstehen oder von technisch gebildeten Interessierten aus diesen Ergebnissen leicht zusammengestellt werden können.

Mechanismen in Hardware gewährleisten einen besseren Schutz, verhindern Piraterie aber keinesfalls perfekt: Alle Hardware-Maßnahmen sind zumindest mittelfristig und bei Massenanwendungen in ihrer Sicherheit gefährdet, da oftmals überraschend einfache Möglichkeiten gefunden werden, die Sicherheit zu unterlaufen und bisher keine langfristig erprobten, für den Massenmarkt geeigneten Techniken zur Verfügung stehen. Zudem stellt sich die Frage, was Konsumenten motivieren sollte, diese Hardware zu erwerben oder auch nur zu nutzen.

Trotz ihrer weit gehenden Unwirksamkeit für den intendierten Zweck neigen Maßnahmen zum Schutz von Inhalten dazu, den Konsumenten durch den Anbieter bzgl. der Nutzung überwachbar zu machen. Neben der Frage der Zulässigkeit wirft dies verschärft die Frage der Akzeptanz dieser Maßnahmen durch datenschutzbewusste Konsumenten auf.

Inhaltsverzeichnis

1 Einführung

Für Menschen, die ihren Lebensunterhalt über Lizenzgebühren bestreiten, dürften die Digitalisierung und das Internet ein Segen und ein Fluch zugleich sein. Die Distributionsmöglichkeiten sind global und billig; die Digitalisierung ermöglicht den verlustfreien Transport zum Konsumenten, aber auch die sehr einfache Herstellung und illegale Verbreitung exakt gleicher Kopien, das bedeutet Kopien ohne Qualitätsverlust. Deshalb stellt sich die Frage, ob und wie Piraten daran gehindert werden können, illegale Kopien zu verbreiten. In dieser Studie werden die technischen Zusammenhänge und Möglichkeiten hierfür untersucht und bewertet.

Für eine Bewertung in Frage kommende Kriterien, teilweise nichttechnischer Natur, sind der Aufwand (speziell die Kosten und die Akzeptanz beim Konsumenten) und die Stärke (speziell gegen welche Stärke eines Angreifers/Piraten ein Schutzsystem noch hilft). Weitere Kriterien sind die Überwachbarkeit der Konsumenten sowie die Frage, wie technische Vorkehrungen das ungehinderte, legale Verbreiten von Kulturgütern beeinflussen.

Die Produkte von Autoren (auch Komponisten, Musikern, Filmproduzenten und Softwareentwicklern) zeichnen sich im Vergleich zu anderen Wirtschaftsgütern durch besonders niedrige Marginalkosten aus. Der Preis des Endproduktes besteht in erster Linie aus dem Autorenhonorar, Aufwendungen für Marketing, der Gewinnspanne für das Vertriebsnetz, sowie einer Risikoabsicherung für den ausstehenden Erfolg des Produktes. Die reinen Herstellungs- und Vertriebskosten einer einzelnen Kopie solcher geistiger Werke fallen in einer Endpreiskalkulation nur unwesentlich ins Gewicht. Ohne einen speziellen Schutz gegen die Nachahmung geistiger Produkte durch Konkurrenten wäre deren Produktion daher kaum mit der Aussicht auf attraktiven nachhaltigen finanziellen Gewinn verbunden. Das Ergebnis wäre ein Kulturangebot, welches in erster Linie von nicht-professionellen Autoren geschaffen wird, deren Erwerbstätigkeit nicht im Wesentlichen in der Schaffung geistiger Werke besteht.

Es besteht daher seit langem in der kulturinteressierten Bevölkerung Europas ein breiter Konsens, dass die rechtliche Einschränkung der Vervielfältigung im Interesse der Aufrechterhaltung eines reichhaltigen professionell produzierten kulturellen Angebotes wünschenswert ist. Daraus haben sich im Laufe der letzten beiden Jahrhunderte die einschlägigen nationalen Urheberrechtsgesetzgebungen und entsprechendes internationales Recht entwickelt.

Der bislang bestehende Schutz gegen die nichtautorisierte Nutzung und Vervielfältigung geistiger Werke nutzt in erster Linie den Umstand, dass zur qualitativ hochwertigen Vervielfältigung und Verteilung erhebliche Produktionsmittel (Druckereipressen, Schallplatten- oder CD-Pressen, Filmkopieranlagen, Lastwagen, Läden, etc.) notwendig sind, deren Betreiber vergleichsweise einfach auf die Einhaltung der Urheberrechtsgesetze hin kontrolliert werden konnten. Jede neue technische Entwicklung zur Vervielfältigung und mehrfachen Nutzung von Informationen und damit möglicherweise auch geistigen Werken wurde von der kulturschaffenden Industrie in der Vergangenheit stets mit Sorge verfolgt, so etwa öffentliche Bibliotheken, Radios, Fernseher, Tonbandgeräte, Bürokopierer, Magnetbandkassetten, Videorecorder, Datenfernübertragung, etc. Die Kulturindustrie reagierte auf diese Entwicklungen in erster Linie mit der

kontinuierlichen Einführung von Medien höherer Qualität (70-mm-Film mit Dolby-Surround Sound statt Videorecorder und Fernseher, CD statt Magnetbandkassette und FM-Radio), um sich für die Kunden in der Produktattraktivität deutlich von den immer weniger kontrollierbaren für Privatpersonen weitverfügbaren Vervielfältigungsmedien zu unterscheiden.

Da diese Qualitätsunterschiede immer geringer werden, steigt gleichzeitig auch die Attraktivität illegaler Kopien. Die Digitalisierung in Verbindung mit der weiten Verbeitung des Internet führte somit zu einer derartigen Verschärfung der Situation, dass sich Technologieunternehmen verstärkt mit der Entwicklung spezieller Sicherheitstechnologie zum Schutz digitaler Inhalte beschäftigten. Diese Technik soll dann die Rechte an digitalen Inhalten verwalten helfen. Neuerdings werden solche Systeme auch Digital-Rights-Management-Systeme (DRM-Systeme) genannt.

1.1 Digital Rights Management (DRM)

Die folgende Begriffsbestimmung für DRM-Systeme ist an [4, S.2ff] angelehnt:

DRM-Systeme sind elektronische Vertriebssysteme für digitale Inhalte. Sie ermöglichen die sichere Verbreitung digitaler Inhalte – unter anderem urheberrechtlich geschützte Musik-, Film- oder Sprachwerke – im Online- und Offline-Bereich, z.B. über das Internet, Datenträger (CompactDisc, MiniDisc etc.), mobile Abspielgeräte oder Mobiltelefone.

DRM-Systeme ermöglichen den Rechteinhabern einen sicheren Vertrieb zu berechtigten Nutzern, eine effektive und differenzierte Rechteverwaltung, weitgehende Kontrolle über die Verbreitung und Nutzung digitaler Inhalte und eröffnen so neue Nutzungsarten und Geschäftsmodelle (z.B. kostenpflichtiger Download, Abbonement von Inhalten, Pay-per-view/listen, file sharing).

In ihrer unflexibelsten Form verhindern DRM-Systeme, dass der Nutzer einen digitalen Inhalt kopieren kann. In ihrer flexibelsten Form erlauben DRM-Systeme die individuelle Abrechnung und Nutzung digitaler Inhalte ähnlich den Telefongebühren.

In DRM-Systeme werden auch Hoffnungen bezüglich der Reformierbarkeit des im Jahre 1965 eingeführten Pauschalabgabesystems für Datenträger und Kopiervorrichtungen gesetzt. Wenn Werke mittes DRM-Systemen geschützt werden können (Kopierschutz) und deren Nutzung individuell vergütet werden kann, seien die alten Pauschalabgabesysteme überflüssig geworden, argumentieren die Technologie-Provider, beispielsweise die Hersteller von CD-Brennern und die Anbieter von DRM-Verfahren.

Die alten Vergütungsmodelle haben ihren Ursprung in der damaligen Erkenntnis des Gesetzgebers, dass mit der Verbreitung privater Vervielfältigungstechniken (damals Tonbandgeräte und Kassettenrecorder) dem Endverbraucher die Nutzung geschützter Inhalte vornehmlich durch Rundfunkmitschnitte ermöglicht wird, die weder verhindert noch kontrolliert werden kann. Kopien waren aufgrund der Analogtechnik stets von minderer Qualität (verglichen mit dem Original). Mit der Digitalisierung und der breiten, kostengünstigen Verfügbarkeit digitaler Kopiertechnik (insbesondere CD-Brenner in PCs) erreicht eine Kopie jedoch exakt die Qualität des Originals. Hinzu kommt noch, dass mit Scannern, Farbdruckern und Spezialpapier heute sogar die CD-Booklets hochqualitativ reproduziert werden können.

Obwohl inzwischen auch DRM-Systeme verfügbar sind, die die gesamte Vertriebskette digitaler Inhalte abdecken, haben sie sich bisher noch nicht breit durchsetzen können. So fehlt es noch an passenden Geschäftsmodellen für die modernen Distributionsformen über das Internet. Dabei bietet gerade der Vertrieb über das Internet realistische Chancen für die schnellere, kostengünstigere und kundenorientiertere Verbreitung von Inhalten. Zumindest dürfte es an mangelnder technischer Kompetenz der Internetnutzer nicht scheitern: Wer es mit einer gehörigen Portion Enthusiasmus und Geduld schafft, über Peer-to-Peer-Filesharing-Systeme (siehe Abschnitt 3.6.2) kostenlos Musik herunterzuladen, wird auch keine Mühe haben, ein ansprechend gestaltetes, effizientes und gut bedienbares Bezahlsystem für digitale Inhalte zu nutzen. Ausserdem haben die Systeme zum kostenlosen File-Sharing ein hohes Image bei den Benutzern. Dieses Potential an Kundeninteresse und Kundenbindung ließe sich sicher auch bei einem Wechsel in die Legalität und Kommerzialisierung erhalten.

Die DRM-Techniken sind meist proprietär und noch nicht breit etabliert, und die Rechteinhaber (Künstler, Medienkonzerne) scheuen sich noch davor, eine bestimmte Technik zu lizenzieren. Aufgrund schlechter Erfahrungen im Bereich Datenträger- und Medienformate (beispielsweise existierten in der Anfangszeit der Heim-Videotechnik wenigstens drei Formate, von denen sich VHS im Heimbereich durchgesetzt hat) ist dieses Abwarten auch verständlich.

1.2 Ausgangslage aus technischer Sicht

Die folgenden Abschnitte analysieren die Ausgangslage und die daraus resultierenden Konsequenzen für die Entwicklung technischer Mechanismen zum Schutz digitaler Inhalte und zeigen technische Trends auf.

1.2.1 Technische Entwicklungen

In den vergangenen zehn Jahren erfolgten erneut eine ganze Reihe sich gegenseitig ergänzender enormer technischer Entwicklungen, die neue Vervielfältigungsmöglichkeiten geistiger Werke bieten und von der Kulturindustrie mit großer Sorge beobachtet werden:

- Frei programmierbare Universalcomputer (PCs) sind ein erschwingliches und populäres Haushaltsgerät geworden. Das anhaltend exponentielle Wachstum der Speicher- und Rechenleistung und die modulare Erweiterbarkeit erlaubt es, auf diesen Geräten heute Funktionen einfachst in Software zu realisieren, für die wenige Jahre zuvor noch sehr teuere spezielle Industrieausrüstung notwendig war.
- Die Digitalisierung des Telefonnetzes sowie die Entwicklung hochleistungsfähiger Glasfaser- und Kupferübertragungstechniken schaffte die Grundlage für den kostengünstigen und einfachen Zugang der gesamten Bevölkerung zu einer universell nutzbaren weltweiten digitalen Datenübertragungs- und Datenarchivierungs-Infrastruktur, dem Internet.
- Forschungsergebnisse in den Bereichen digitale Signalverarbeitung, Informationstheorie und Sinnesphysiologie ermöglichten die Entwicklung hocheffizienter Kodierverfahren für Bild- und Tonsignale (z.B. ISO MPEG), welche die Übertragung und Speicherung derartiger Daten zehn bis hundertfach effizienter gestalten als herkömmliche Distributionsformate.

- Die Unterhaltungselektronik- und Computerindustrie amortisierte die enormen Entwicklungs- und Investitionskosten für neue Speicher- und Übertragungstechnologien (CD, DVD, Firewire) durch Einsatz der gleichen Formate sowohl für den Vertrieb von geistigen Produkten als auch als Universalmedien für den Computergebrauch.

- Die dezentrale, oft nicht-kommerzielle, schnell-lebige und internationale Natur vieler über das Internet erreichbarer Dienste erschwert die Durchsetzung gesetzlicher Urheberrechtsbestimmungen, was sich insbesondere durch die derzeit noch im frühen Anfangsstadium befindliche Entwicklung anonymer und zensurresistenter Publikationsdienste verschärfen dürfte.

1.2.2 Konsequenzen

Das Ergebnis dieser Entwicklung ist, dass heute selbst technisch wenig versierten Privatleuten Haushaltsgeräte zur Verfügung stehen, mit denen geistige Werke effizient, bequem und ohne Qualitätsverlust vervielfältigt, archiviert, indiziert, gesucht und weltweit übertragen werden können. Betroffen davon sind insbesondere Musikaufnahmen in CD-Qualität, die heute auf eine Datenrate von 120–160 kbit pro Sekunde komprimiert werden können (MPEG Audio Layer 3) um dann mit etwa 60 kbit pro Sekunde über das Telefonnetz übertragen zu werden (ISDN, V.92). Damit beträgt die Ladezeit von Musik über das Internet derzeit etwa das doppelte der Spielzeit.

Verbesserte Kodierverfahren (z.B. MPEG-2 AAC+SBR) ermöglichen inzwischen über das Telefonnetz gar eine der Spielzeit entsprechende Ladezeit. Verbesserte und für Privathaushalte erschwingliche Internetzugangstechnologien (ADSL, Kabelmodems) verkürzen die Ladezeit weiter um einen Faktor 5–30. Zunehmend kritisch wird der Schutzbedarf für digitalisierte Kinofilme, da die typischen Filmlängen (90 min) und wesentlich höhere Datenraten von 4000–8000 kbit pro Sekunde zwar noch relativ lange Ladezeiten erfordern. Raubkopien von DVDs können allerdings bereits heute mit erträglichen Qualitätseinbußen auf einer CD-R untergebracht werden. Perfekte Raubkopien können jedoch künftig auch in Form von DVD-RW Medien in Umlauf gebracht werden.

Aufgrund der weiten Verfügbarkeit von Software-Entwicklungswerkzeugen für Heimcomputer sind heute frei verfügbare und privat entwickelte Kopier- und Abspielprogramme oft deutlich weiter entwickelt und schneller verfügbar, als dies die vergleichsweise langen Produktzyklen der etablierten Unterhaltungselektronikindustrie erlauben würden. Über das Internet finden sich heute schnell Gruppen von enthusiastischen Hobbyentwicklern zusammen, die derartige Systeme ohne kommerzielle Interessen gemeinsam entwickeln, verbessern und der Allgemeinheit frei zur Verfügung stellen. Produktzyklen für frei verfügbare Kopierhilfssoftware werden in Wochen statt wie im kommerziellen Bereich in Jahren oder Jahrzehnten gemessen.

Der Kampf gegen die illegale Bereitstellung und Nutzung urheberrechtlich geschützter Daten im Internet mit Hilfe technischer Mittel scheint angesichts der phantasievollen Umgehungsmöglichkeiten von Sperren aussichtslos. Die Markierung geschützter Inhalte mit Hilfe digitaler Wasserzeichen und digitaler Fingerabdrücke ermöglicht wenigstens die Verfolgung individuell markierter Kopien und besitzt damit für den Piraten abschreckende Wirkung.

Eine Verbreitung von digitalen 1:1-Kopien könnte mit Hilfe hardwaregestützter kryptographischer Verfahren verhindert werden. Allerdings sind solche Techniken sehr teuer und helfen in

der Praxis sehr wahrscheinlich auch nur eine begrenzte Zeit. Versuche, das Internet dermaßen zu verändern, dass die Benutzer bei allen Handlungen (egal, ob legal oder illegal) verfolgbar sind, scheitern technisch an der Verfügbarkeit und Nutzbarkeit von Anonymisierungsdiensten und dürften zudem in Konflikt stehen mit datenschutzrechtlichen Bestimmungen.

Kommunikation findet heutzutage über offene Netze statt. Das bedeutet, man hat sich auf wesentliche technische Standards zur Kommunikation geeinigt, deren Verwendung nicht durch Patente, Lizenzen o. ä. eingeschränkt wird. Das Internet ist ein solches offenes Netz. Die verteilte Netzstruktur des Internet besteht aus Rechnern vieler verschiedener Hersteller mit sehr unterschiedlicher Hardware- und Softwareausstattung, was die technische Offenheit unterstreicht. Damit die daraus resultierende Vielfalt kein Hindernis bei der weltweiten Kommunikation ist, wurden technische und organisatorische Kommunikationsvereinbarungen getroffen, an die sich alle Rechner des Internet halten müssen.

Die Vielfalt an Benutzern und Betreibern hat weiterhin die Konsequenz, dass man nicht davon ausgehen kann, dass sich alle Akteure im Internet kooperativ verhalten. Es existiert zwar eine sog. Netiquette, aber niemand ist gezwungen, sich daran zu halten. Nicht kooperatives Verhalten wird durch das Internet größtenteils noch nicht verhindert. Anders herum gesagt: Es existieren derzeit nur sehr wenige Sicherheitsfunktionen, die Betreiber und Benutzer vor Angriffen auf die Verfügbarkeit, Integrität, Zurechenbarkeit und Vertraulichkeit von Diensten und Daten schützen. Dieses Defizit muss für die ernsthaft geschäftsmäßige Anwendung des Internet, also für E-Business, beseitigt werden, sonst leidet auf lange Sicht die Vertrauenswürdigkeit eines „im Netz“ agierenden Unternehmens.

1.2.3 Technische Trends

Derzeit sind einige Trends zu beobachten, die auch ihre Auswirkungen auf Techniken zum Schutz digitaler Inhalte haben:

- **Konvergenz der Systeme:** Die Hersteller von Soft- und Hardware gehen zunehmend dazu über, mit einem einzigen System möglichst viele Formate, Standards, Kodierungen etc. zu unterstützen. Beispielsweise unterstützt Quicktime von Apple heute über 50 verschiedene Grafik-, Sound- und Videoformate. Set-Top-Boxen unterstützen teilweise mehrere Schutzsysteme (Multicrypt). Umgekehrt werden die gleichen Inhalte gleich für mehrere unterschiedliche Schutzsysteme ausgestrahlt, um sie auch auf verschiendenen Typen von Empfangsgeräten nutzen zu können (Simulcrypt). Die beiden Varianten sind in Abbildung 1.1 gegenübergestellt.

- **Schaffung von Plattformen:** Set-Top-Boxen werden universell. Personal Computer und Fernseher werden technisch immer ähnlicher. Mit der Multimedia Home Platform (MHP) verschmelzen beide Welten derart miteinander, dass technische Unterschiede kaum noch auszumachen sind.

- **Standardisierung:** Da proprietäre Systeme stets eine begrenzte Marktdurchdringung haben und für den Verbraucher wenig Nutzen bringen, soll nun über offene Standards versucht werden, gemeinsam den Durchbruch zuschaffen. MHP ist beispielsweise europaweit durch ETSI (European Telecommunications Standards Institute) standardisiert.

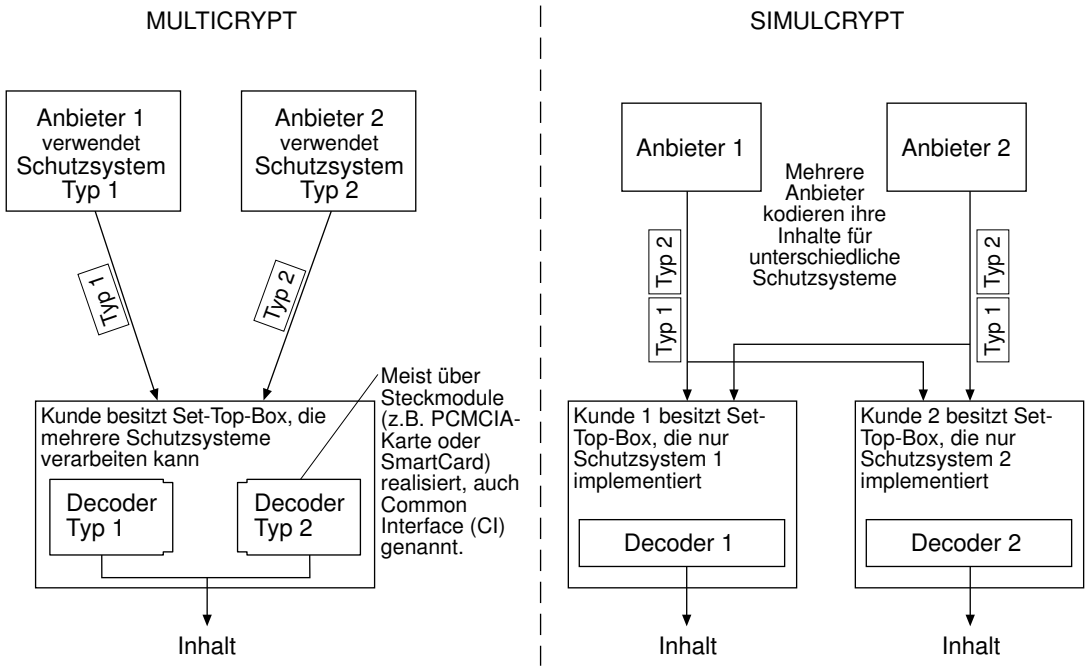

Abbildung 1.1: Gegenüberstellung von Multicrypt und Simulcrypt

1.3 Technische Grundlagen

Die folgenden Abschnitte vermitteln einige Grundlagen der IT-Sicherheit, benennen die heute üblichen Basistechniken der IT-Sicherheit, führen in die Grundverfahren der Distribution multimedialer Inhalte ein und erläutern kurz die heute üblichen Übertragungsprotokolle im Internet.

1.3.1 Schutzgüter, Bedrohungen und Schutzziele

In komplexen IT-Systemen, wie es unsere heutigen und zukünftigen Kommunikationsnetze sind, handeln verschiedene Subjekte (Organisationen, Personen). Sie können dabei nicht nur kooperieren, sondern auch konkurrieren (z. B. um Betriebsmittel), sabotieren (z. B. Kommunikation behindern, stören, blockieren, lahmlegen), fingieren (z. B. Identitäten vortäuschen, Daten verändern) oder abhören (z. B. bespitzeln, lauschen). Die Großrechner vor 25 Jahren waren streng bewacht, d.h. für sie galten Zugangskontrollmaßnahmen (Pförtner, Stahltüren etc.), die nicht leicht zu überwinden waren. Die Vernetzung von Rechnern blieb Spezialanwendungen vorbehalten.

IT-Systeme (einschließlich der Übertragungsstrecken) müssen außerdem gegen unbeabsichtigte Fehler und Ereignisse (z. B. höhere Gewalt, technische Fehler, Fahrlässigkeit, Programmierfehler, Verschleiß, Havarien) und beabsichtigte Angriffe (z. B. Abhören, Manipulation und Zerstören von Informationen, aber auch von Software und Hardware) von außen (z. B. Hacker oder Terroristen mit Sprengstoff) und innen (z. B. Administratoren, Programmierer) gesichert werden.

Seit den frühen 80er Jahren [55] findet sich eine Dreiteilung der Bedrohungen und korrespondierenden **Schutzziele** Vertraulichkeit, Integrität und Verfügbarkeit:

- Unbefugter Informationsgewinn, d.h. Verlust der **Vertraulichkeit** (Confidentiality),
- Unbefugte Modifikation von Informationen, d.h. Verlust der **Integrität** (Integrity) und
- Unbefugte Beeinträchtigung der Funktionalität, d.h. Verlust der **Verfügbarkeit** (Availability).

Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern. Entsprechend lassen sich die großen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit verfeinern.

	Inhalte Worüber?	Umfeld Wer, wann, wo, mit wem, wie lange?
Unerwünschtes verhindern	Vertraulichkeit von Nachrichteninhalten	gegenseitige Anonymität der Anwender
	Verdecktheit von Nachrichteninhalten	Unbeobachtbarkeit der Anwender durch die Betreiber
Erwünschtes leisten	Integrität von Nachrichteninhalten	Zurechenbarkeit von Nachrichten zu Absendern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Tabelle 1.1: Gliederung von Schutzzielen

Sicherheit zu realisieren bedeutet, sich gegen einen **intelligenten Angreifer** bestimmter Stärke schützen zu können. Dieser Angreifer wird im Angreifermodell charakterisiert: Ein **Angreifermodell** definiert die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus (z.B. ein ganz bestimmtes Verschlüsselungsverfahren) gerade noch sicher ist. Dabei berücksichtigt das Angreifermodell folgende Aspekte:

1. Aktive oder passive Rolle des Angreifers:
   - Was kann der Angreifer maximal passiv beobachten?
   - Was kann der Angreifer maximal aktiv kontrollieren (steuern, verhindern) bzw. verändern?
2. Mächtigkeit des Angreifers:
   - Wieviel Rechenkapazität besitzt der Angreifer?
   - Wieviel finanzielle Mittel besitzt der Angreifer?
   - Wieviel Zeit besitzt der Angreifer?
   - Welche Verbreitung hat der Angreifer? Oder spezieller: Welche Leitungen, Kanäle, Stationen kann der Angreifer beherrschen?

Als potentielle Angreifer können Außenstehende, Teilnehmer, Betreiber, Hersteller, Entwickler und Wartungstechniker betrachtet werden, die natürlich auch kombiniert auftreten können. Außerdem kann man nach Angreifern innerhalb des betrachteten IT-Systems (Insider) und außerhalb (Outsider) unterscheiden. Die Feststellung, dass eine Instanz angreifen kann, ist nicht gleichzusetzen damit, dass sie wirklich angreift.

Grundsätzlich gilt: Man sollte einem Angreifer nie zuwenig zutrauen. Die Kosten, die ein Angreifer zum Knacken eines Systems aufwenden wird, müssen aber selbstverständlich in einem gesunden Verhältnis zu den Kosten des Schutzes stehen. Insofern mag ein Schutzmechanismus, der gegen einen „Gelegenheitstäter“ etwas hilft, aber nicht gegen einen professionellen Knacker, durchaus sinnvoll sein, wenn die Verluste hauptsächlich durch den Gelegenheitstäter auftreten. Die globale Verfügbarkeit von Informationen und automatisierten Tools im Internet lässt aber zunehmend die Grenzen zwischen Amateur und Profi verschwimmen, weshalb in der Praxis von einem starken Angreifer ausgegangen werden sollte.

In letzter Konsequenz heißt das: Experten werden Tools entwickeln, die jedermann in die Lage versetzen, gegen Copyright wie auch DRM-Techniken zu verstoßen, und dies vermutlich so, dass es der Enduser gar nicht merkt.

1.3.2 Basistechniken zum Schutz

Um die Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit in informationstechnischen Systemen zu realisieren, existieren Basismechanismen, die heute gut erforscht und teilweise auch benutzerfreundlich einsetzbar sind.

Die Vertraulichkeit von Nachrichten kann mit Hilfe von **Verschlüsselung** erreicht werden. **Message Authentication Codes** dienen dem Schutz von Nachrichten vor unerkannter Verfälschung auf den Übertragungswegen.

Mit Hilfe der **digitalen Signatur** ist Zurechenbarkeit realisierbar: Nachrichten können so ihrem „Unterzeichner“ eindeutig zugeordnet werden.

Die Anonymität und Unbeobachtbarkeit von Internet-Nutzern kann durch sog. **datenschutzfreundliche Techniken** realisiert werden. Im Bereich E-Commerce sind die bekanntesten Verfahren, die zur Klasse der anonymen Verfahren zählen, die digitalen anonymen Zahlungssysteme und Verfahren zum unbeobachtbaren Web-Surfen im Internet.

Die Verfügbarkeit von Daten und Diensten kann erreicht werden durch **Diversität und redundante Auslegung** von Leitungskapazitäten, Rechenressourcen und Datenspeichern.

Eine ausführliche Darstellung der Basistechniken zum Schutz vor intelligenten Angreifern ist z.B. in [20] zu finden.

Neben den Verschlüsselungsverfahren haben für den Bereich Digital Rights Management spezielle Techniken zum Schutz der Inhalte eine hohe Bedeutung. In Kapitel 2 werden die dort angewendeten Techniken vorgestellt.

1.3.3 Distribution von multimedialen Inhalten

Man kann Verteilung von multimedialen Inhalten unterscheiden nach Offline-Verteilung, z.B. über Compact Disc oder andere Datenträger und Online-Verteilung, z.B. per Rundfunk, über spezielle Verteilkabel, Telefon oder über das Internet.

	Online	Offline
Synchron	z.B. Rundfunk, Fernsehen, Webcasting, Simulcasting	—
Asynchron	z.B. Abruf von Webseiten im Internet	z.B. Distribution über Datenträger (CD, DVD)

Tabelle 1.2: Verteilungsformen von Inhalten

Online verteilte Inhalte können synchron und asynchron konsumiert werden. Synchron/asynchron bezieht sich auf den zeitlichen Zusammenhang zwischen Datenübertragung und Konsumierung (Tabelle 1.2).

- **Asynchron:** Inhalte, die auf einem Datenträger verteilt werden, können zu jeder beliebigen Zeit und auch mehrmals konsumiert werden.
- **Synchron:** Inhalte, die synchron übertragen werden (z.B. Rundfunk, Fernsehen, aber auch Streaming-Daten im Internet), müssen vom Konsumenten erst gespeichert werden, damit sie asynchron oder wiederholt konsumiert werden können.

Bei der synchronen Online-Übertragung im Internet unterscheidet man neuerdings noch nach Simulcasting und Webcasting. Unter Simulcasting wird die zeitgleiche Übertragung von terrestrischen Sendungen im Internet verstanden, während mit Webcasting die Nur-Internet-Übertragung gemeint ist.

Neben Offline/Online kann man auch nach der Eignung des Mediums zur Interaktivität unterscheiden. Interaktive Inhalte besitzen heute meist (aber nicht notwendigerweise) eine Online-Komponente.

Weiterhin ist zu unterscheiden, ob alle Konsumenten exakt gleiche Kopien des Inhaltes erhalten oder ob sie individualisierte, d.h. speziell auf sie zugeschnittene Kopien (z.B. mit eingebetteten Informationen über Kaufdatum, Besitzer etc.) erhalten. Die individualisierte Verteilung der Inhalte ist offline schwer bzw. nicht möglich und kann deshalb momentan praktisch nur für den Online-Abruf (ggf. mit anschließender erlaubter Speicherung des Inhalts) realisiert werden.

Bei der Distribution von Inhalten im Internet (egal, ob synchron oder asynchron) werden heute meist exakt gleiche Kopien an alle Konsumenten übermittelt.

Synchrone und asynchrone Distributionsformen sind von der leichten Kopierbarkeit im gleichen Maße betroffen, da es einfach möglich ist, die Inhalte digital aufzuzeichnen und ebenfalls asynchron (d.h. zeitversetzt) weiterzuverbreiten (siehe auch Abschnitt 3.6.2).

Der Vertrieb von Inhalten fand und findet aufgrund der teilweise unbefriedigenden Übertragungskapazitäten der Online-Anschlüsse privater Haushalte über Datenträger statt. Der Anteil der Online-Verteilung nimmt jedoch stetig zu, insbesondere im Audio-Betreich, wo die Übertragungskapazitäten inzwischen ausreichen.

1.3.4 Übertragungsprotokolle im Internet

Bevor näher auf den Schutz von Daten eingegangen wird, sollen einige Grundbegriffe der Übertragungsprotokolle im Internet eingeführt werden, da deren Verständnis die Voraussetzung für die Beurteilung der praktischen Anwendbarkeit der Schutzmechanismen ist.

Nutzerdaten werden im Internet mit Hilfe von zwei Übertragungsprotokollen transportiert, dem Transmission Control Protocol (TCP) und dem User Datagram Protocol (UDP), siehe Tabelle 1.3.

	TCP	UDP
Punkt-zu-Punkt	Etabliert, Beispiel: HTTP (WWW)	Etabliert, aber teilweise keine Quality-of-Service-Zusicherungen, Beispiel: Real Player
Multicast, Broadcast	—	In Entwicklung und Erprobung

Tabelle 1.3: Übertragungsprotokolle im Internet

Transmission Control Protocol (TCP)

Das Transmission Control Protocol (TCP) wird bei Punkt-zu-Punkt-Verbindungen zwischen zwei Endpunkten, z.B. einem Browser und einem Webserver eingesetzt. Bei TCP wird darauf geachtet, dass alle vom einen Endpunkt gesendeten Bits auch tatsächlich beim anderen Endpunkt ankommen und auch ihre Reihenfolge nicht durcheinander kommt. Falls Daten beim Transport verloren gehen, werden sie erneut gesendet (Retransmission). Dieses Transportprotokoll wird z.B. beim Transport von Webseiten, E-Mails, Dateien etc. angewendet, da man sicher gehen möchte, dass die Daten auch wirklich beim Empfänger ankommen.

Sollen mit Hilfe von TCP-Verbindungen viele Nutzer mit dem gleichen Inhalt von einem Server versorgt werden, muss jeder Nutzer eine eigene Verbindung zum Server aufbauen (Abbildung 1.2). Der Bedarf an Bandbreite wächst dadurch linear mit der Teilnehmerzahl, da der Server jeweils eine Verbindung pro Client und Request unterhält. Selbst wenn mehrmals die gleichen Inhalte vermittelt werden sollen, erfolgt keine Konzentration, etwa um Bandbreite zu sparen. Dass ein solches Vorgehen nicht besonders effektiv ist, liegt auf der Hand, allerdings ist TCP auch nicht unbedingt für solche Verkehrsformen wie Broadcasting gedacht gewesen.

Deshalb wird mit Hilfe einer Replikation des Datenbestandes (die Server R1 und R2, siehe Abbildung 1.3, werden mit Kopien der Inhalte des Servers versorgt) und sog. Caching-Techniken versucht, einen Lastausgleich und bessere Antwortzeiten zu erreichen. Einen solchen Service bietet z.B. die Firma Akamai (http://www.akamai.com/) an.

Die Replikation löst allerdings nicht das Grundproblem der Mehrfachverteilung von Informationen, sondern reduziert es nur, da es trotzdem vorkommen wird, dass mehrere Nutzer gleichzeitig den gleichen Inhalt von einem Server abrufen.

User Datagram Protocol (UDP)

Beim User Datagram Protocol (UDP) sendet der Sender Datenpakete aus. UDP ist ein verbindungsloses Protokoll und wird u.a. im Bereich Streaming angewendet. In Abhängigkeit von der Auslastung des Netzes erreicht dann z.B. ein Datenpaket des Multimedia-Streams den Empfänger rechtzeitig, zu spät (delayed) oder auch gar nicht (dropped). UDP wird

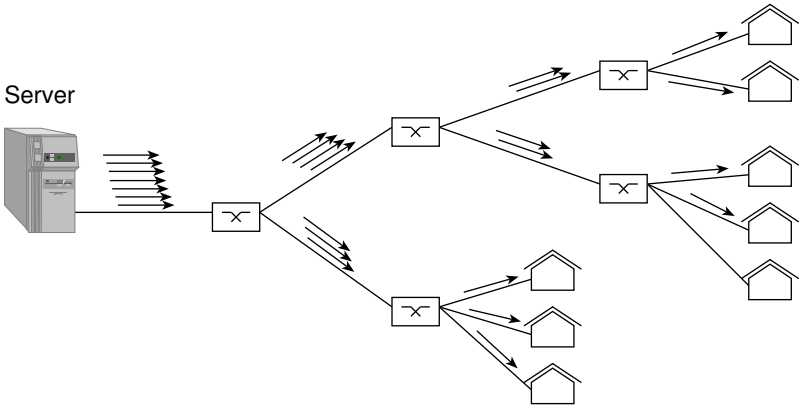

Abbildung 1.2: Punkt-zu-Punkt-Verbindungen

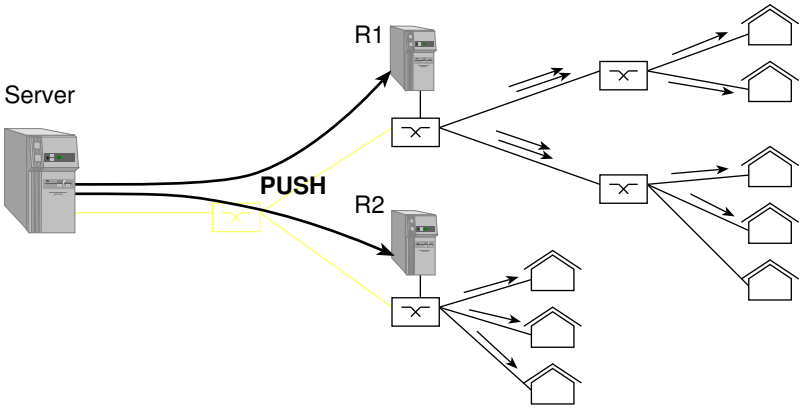

Abbildung 1.3: Replikation des Datenbestandes

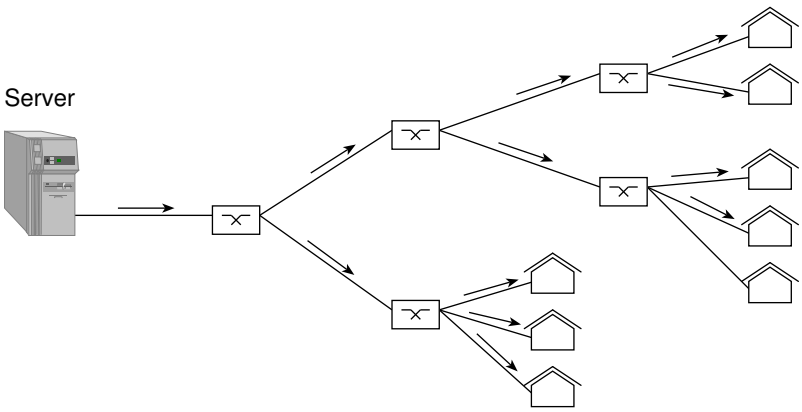

Abbildung 1.4: Multicast von Streamingdaten

hauptsächlich für Datenströme verwendet, bei denen eine Retransmission nicht möglich ist. Beispielsweise bei Audio- und Videoströmen, die synchron gesendet und konsumiert werden, ist es nicht sinnvoll, verloren gegangene Datenpakete erneut zu senden, da der fehlende „Abschnitt“ des Datenstroms zeitlich hinter dem aktuell gesendeten liegt. UDP-Pakete werden beispielsweise vom Real Player (http://www.real.com/) verarbeitet. Der Verlust von Datenpaketen macht sich je nach Kodierung der Medienströme durch Qualitätsverschlechterung oder Aussetzer bemerkbar.

Neben der Punkt-zu-Punkt-Übertragung von UDP-Paketen lassen sich auch Punkt-zu-Mehrpunkt-Übertragungen (Multicast, Broadcast) realisieren. Diese Klasse von UDP-Verkehr soll u.a. den Bereich des Webcasting abdecken (siehe Abbildung 1.4). Dabei verbindet sich ein Benutzer z.B. mit einen Videodatenstrom über eine sog. Multicast-Adresse (join). Dies wird durch das sog. Internet Group Management Protocol (IGMP) realisiert.

Derzeit wird massiv an der Zusicherung sog. Quality-of-Service-Merkmale (QoS) gearbeitet, um die auftretenden Verzögerungen und Datenverluste derart vorhersagen bzw. vermeiden zu können, dass dem Endbenutzer eine gleich bleibend hohe Qualität der Übertragung zugesichert werden kann. Die bisher entwickelten Protokolle tragen Namen wie Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP) und Real-Time Streaming Protocol (RTSP). Im Zusammenhang mit QoS existiert noch ein Resource Reservation Protocol (RSVP). In der gegenwärtigen Distributionspraxis im Internet spielen die genannten Protokolle noch keine große Rolle, was sich aber mit steigenden Übertragungskapazitäten ändern wird. An technischer Einführungsliteratur in die Multicastprotokolle kann [38] empfohlen werden.

2 Techniken zum Schutz

Um die gesetzlich schwierig kontrollierbare unrechtmäßige Verbreitung von schützenswerten Inhalten einzudämmen, wurden eine Reihe von technischen Maßnahmen vorgeschlagen. Eine Kategorisierung der Mechanismen ist schwierig, da die in der Praxis anzutreffenden DRM-Systeme meist eine Kombination mehrerer Mechanismen darstellen.

2.1 Übersicht

Wir verwenden für die Darstellung der Mechanismen folgende Gliederung:

1. **Kerntechniken der IT-Sicherheit, die auch im DRM-Bereich Anwendung finden.**
   - **Verschlüsselung:** Um individualisierte und kostenpflichtige Dienste vor unberechtigter Nutzung zu schützen, müssen die übertragenen Inhalte verschlüsselt sein.
   - **Schutz durch manipulationssichere Hardware:** Sicherheitsmechanismen verwenden (meist kryptographische) Geheimnisse, deren Kenntnis die Voraussetzung für die Nutzung der Inhalte ist. Die einzige derzeit halbwegs sichere Methode zur Aufbewahrung der Geheimnisse ist sog. Tamper-Resistant Hardware.
   - **Schutz durch Software-Kapselung:** Wenn schon keine Tamper-Resistant Hardware eingesetzt werden kann, weil die zu schützenden Inhalte beispielsweise auf einem handelsüblichen PC nutzbar sein sollen, so sollte wenigstens die Ausführungsumgebung, in der das Rechtemanagement erfolgt, gegen böswillige fremde Software (Trojanische Pferde, Sniffing- und Hacker-Software) geschützt sein. Ein Softwareschutz gegen Angriffe durch den Betreiber und Besitzer des Rechners ist dagegen heute aussichtslos.
2. **Speziell für DRM designte halbwegs starke Mechanismen zum Schutz.**
   - **Modifikation des analogen Endsignals:** Selbst wenn man DRM-Systeme so bauen würde, dass nur analoge Signale abgreifbar wären, sollte das Abgreifen und erneute Digitalisieren erschwert werden.
   - **Watermarking:** Damit urheberrechtlich geschützte digitale Mediendaten als solche erkennbar sind und auch nach Manipulationen erkennbar bleiben, werden sie mit digitalen Wasserzeichen versehen.
   - **Fingerprinting:** Für den Schutz der Urheberrechte an multimedialen Inhalten wird man zunehmend dazu übergehen, individualisierte Kopien zu verteilen, um eine Rückverfolgung des illegalen Distributionsweges zu ermöglichen.

3. **Schwache und mittelbar wirksame Mechanismen, die ernsthaften Angriffsversuchen nicht standhalten.**
   - Einbringen von Codes ohne besondere Sicherung,
   - bewusste Schaffung von Inkompatibilitäten, um die Nutzung legaler Inhalte einzuschränken,
   - das Aufspüren von illegalen Inhalten sowie
   - das Sperren bzw. Filtern dieser Inhalte.

Auf die genannten Techniken wird im Folgenden ausführlicher eingegangen.

2.2 Kerntechniken der IT-Sicherheit

In den folgenden Abschnitten werden die kryptographischen Grundverfahren und deren Anwendung für die Verschlüsselung von Inhalten und Medienströmen erläutert. Sichere DRM-Verfahren setzen eine Kapselung des Rechtemanagements voraus, die bevorzugt durch manipulationssichere Hardware oder notfalls durch geschützte Software-Ausführungsumgebungen, sog. Sandboxen, erfolgen sollte.

2.2.1 Kryptographische Grundverfahren

Kryptographie dürfte die mit Abstand ausgereifteste Technik sein, die auch sofort zur Verfügung steht, während die anderen teilweise noch im Entwicklungs- und Einführungsprozess sind. Man unterscheidet symmetrische und asymmetrische Verschlüsselungsverfahren. Wenn sowohl Sender als auch Empfänger über den gleichen kryptographischen Schlüssel verfügen, spricht man von symmetrischen Systemen, andernfalls von asymmetrischen.

Symmetrische Kryptosysteme

Die bekanntesten und ältesten kryptographischen Systeme sind symmetrische Systeme (siehe Abbildung 2.1). Ihre bekanntesten Vertreter sind DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) und AES (Advanced Encryption Standard).

Wenn eine Nachricht x verschlüsselt über einen unsicheren Kanal gesendet werden soll, muss der Schlüssel k bei Sender und Empfänger vorliegen. Für den Distributionsweg eines Inhaltes bedeutet dies, dass der Inhalt verschlüsselt verbreitet wird und beim Empfänger im Endgerät entschlüsselt wird. Um zu verhindern, dass der Empfänger unverschlüsselte digitale Kopien anfertigen und weiter verbreiten kann, muss u.a. der Schlüssel besonders gesichert, d.h. vor Kenntnisnahme durch den Empfänger geschützt, sein. Zusätzlich muss selbstverständlich auch das Abgreifen des unverschlüsselten digitalen Inhalts unmöglich gemacht werden. Als sicherheitstechnisch befriedigende Lösungen kommen hier nur Hardware-Lösungen (sog. Tamper-Resistant Hardware, siehe Abschnitt 2.2.3) in Betracht. Ein Softwareschutz ist völlig unsicher und kann mit sehr geringem Aufwand gebrochen werden. Die Konsequenz ist, dass der Schlüssel nach Bekanntwerden bei *allen Empfängern* ausgewechselt werden muss, was in der Praxis nahezu unmöglich ist.

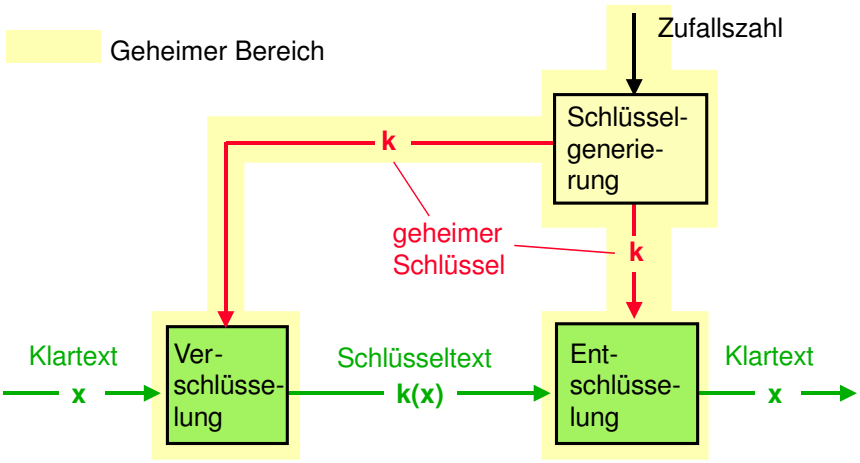

Abbildung 2.1: Symmetrisches kryptographisches System

Asymmetrische Kryptosysteme

Die bekanntesten asymmetrischen Systeme (siehe Abbildung 2.2) sind RSA und ElGamal (jeweils benannt nach ihren Erfindern Rivest, Shamir, Adleman bzw. ElGamal). Im Vergleich zu symmetrischen Kryptosystemen sind sie deutlich rechenaufwendiger (etwa Faktor 100 bis 1000).

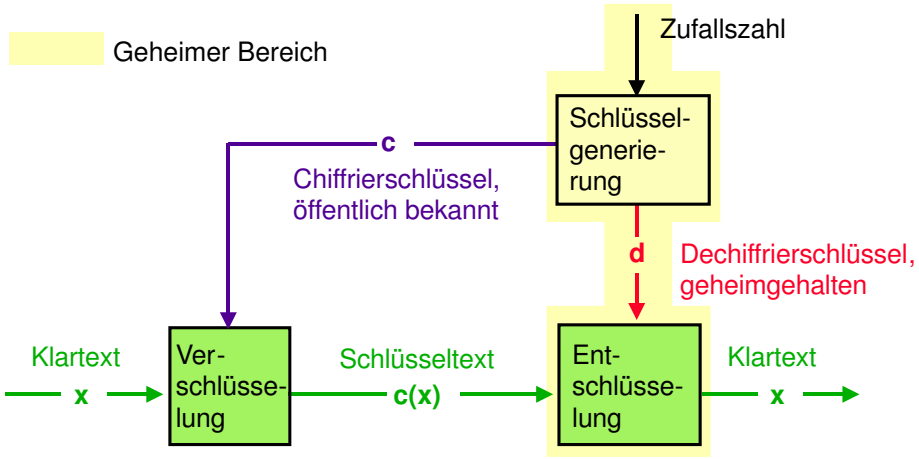

Abbildung 2.2: Asymmetrisches kryptographisches System

Asymmetrische Systeme wurden erfunden, um die Schlüsselverteilung zu vereinfachen. Hier sind zum Ver- und Entschlüsseln verschiedene Schlüssel *c* und *d* erforderlich, und nur *d* muss geheimgehalten werden. Damit man *c* tatsächlich nicht geheimhalten muss, darf *d* nicht mit vernünftigem Aufwand aus *c* zu bestimmen sein.

Hybride Kryptosysteme

Asymmetrische Systeme werden meist eingesetzt, um einen symmetrischen Session Key zu verschlüsseln und zum Teilnehmer zu übertragen (sog. hybride Kryptosysteme). Der Teilneh-

mer entschlüsselt den Session Key und verwendet ihn, um den Medienstrom, der seinerseits mit dem Session Key verschlüsselt wurde, wieder zu entschlüsseln. Die Konsequenz für die Distribution von Inhalten ist, dass jetzt *zusätzlich* vor der Übertragung der Inhalte an *jeden* der Sitzungsschlüssel gesendet werden muss. Dieses Vorgehen ist zwar aufwendiger, hat aber für die Online-Distribution folgende Vorteile:

1. Ein regelmäßiger Schlüsselwechsel ist möglich. Ein in der Vergangenheit kompromittierter Sitzungsschlüssel nützt dem Unberechtigten nur etwas bis zum nächsten Schlüsselwechsel.

2. Eine individualisierte Verteilung der Sitzungsschlüssel ist möglich, d.h. individualisierte Zugänge zu bestimmten Inhalten (On-Demand-Dienste) sind realisierbar.

Ersteres ist auch mit einem symmetrischen Schlüssel zur Session-Key-Verteilung möglich. Anstelle des asymmetrischen Schlüssels wird jedem Teilnehmer ein symmetrischer Schlüssel zugeordnet, mit dem der Session Key verschlüsselt wird. Dies ist in der Praxis meist effizienter, weil asymmetrische Verfahren rechenaufwendiger sind und bei sehr wenig zu übertragenden Bits zu einer Nachrichtenexpansion führen. Außerdem erhält der Empfänger den Schlüssel sowieso vom Sender, so dass der vereinfachte Schlüsselaustausch asymmetrischer Systeme nicht zum Tragen kommt.

Zweites ist auch einfacher mit anderen Techniken, z.B. dem Übertragen von individuellen Seriennummern (Freischalt-Codes), die das individuelle Freischalten der Inhalte nach Bezahlung übernehmen, möglich. Anstelle des Wechsels des Sitzungsschlüssels wird der Medienstrom stets mit einem festen Schlüssel verschlüsselt. Sobald die Abspiel-Hardware einen individuellen Freischalt-Code empfängt, entschlüsselt sie die Inhalte und gibt sie unverschlüsselt an das Ausgabegerät (Bildschirm, Lautsprecher etc.) weiter.

Geheimgehaltene Systeme

Insbesondere dann, wenn Sicherheitsmechanismen von Entwicklern entworfen werden, deren Kerngebiet nicht Sicherheit ist, sondern z.B. Nachrichtenformate, Kommunikationsprotokolle, Geräte- und Mediendesign (kurz: Laien auf dem Gebiet Sicherheit), entstehen meist proprietäre, d.h. nicht standardisierte Schutzmechanismen. Um einen vermeintlich besseren Schutz zu erzielen, wird das Design der Sicherung geheim gehalten. Dies bedeutet nicht zwangsläufig einen Sicherheitsgewinn, sondern kann umgekehrt zu einem Sicherheitsverlust führen, weil beim Design wichtige Angriffe übersehen wurden und dies zunächst niemand bemerkt. Später könnte erfolgreiches Reverse Engeneering (siehe Abschnitt 3.4) plötzlich zur Unsicherheit der gesamten im Einsatz befindlichen Technik führen.

Die Sicherheit des Verfahrens soll, wie es für gute Verschlüsselungsverfahren gilt, nur durch die Geheimhaltung eines kryptographischen Schlüssels erzielt werden. Daraus ergibt sich die Forderung, dass jeder Schutzmechanismus, der ernst genommen und auch rechtlichen Auseinandersetzungen stand halten soll, vollständig offen gelegt und seine Qualität durch Experten bestätigt sein muss. Ist man sich als Anbieter von Sicherheitstechnik seiner Sache jedoch sehr sicher und sind rechtliche Auseinandersetzungen nicht zu erwarten, kann Geheimhaltung des Designs eine zusätzliche Hürde für den Angreifer darstellen.

2.2.2 Verschlüsselung von Inhalten und Medienströmen

Die im vorangegangenen Abschnitt eingeführten kryptographischen Verfahren sollen nun für die Verschlüsselung von Inhalten in Online-Verbindungen und auf Datenträgern angewendet werden.

Verschlüsselung von Online-Verbindungen

Heutzutage existieren auch für den Schutz von Inhalten beim Streaming und Abruf über Netze derart ausgereifte Verschlüsselungsverfahren, dass bei richtiger Anwendung das Knacken der Verschlüsselung praktisch unmöglich ist. Für individualisierte und insbesondere kostenpflichtige Dienste sollten also, wann immer möglich, die Mediendaten verschlüsselt werden, um sie vor unberechtigtem Zugriff auf den Übertragungswegen zu schützen (Abbildung 2.3).

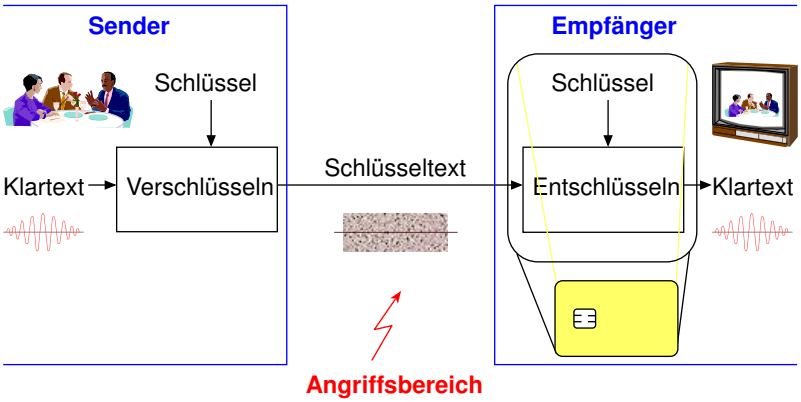

Abbildung 2.3: Verschlüsselung auf Übertragungswegen

Die individuelle Verschlüsselung (d.h. jeder Kunde besitzt einen anderen Schlüssel) hat allerdings den Nachteil, dass jeder Kunde einen anderen Medienstrom erhalten müsste, was wiederum mit einer enormen Verschwendung an Übertragungskapazität verbunden wäre (vgl. auch Abbildung 1.2), zumindest wenn alle Kunden zeitgleich mit den gleichen Mediendaten versorgt werden sollen.

In der Praxis wird deshalb meist ein einziger verschlüsselter Medienstrom übertragen. Alle Kunden erhalten den gleichen Schlüssel, der sich z.B. in einer Chipkarte oder in einer Set-Top-Box befindet und der das Gerät nie verlässt. Andernfalls wäre die illegale Verbreitung des Schlüssels möglich. Mit diesem Schlüssel kann dann ein temporär gültiger Sitzungsschlüssel entschlüsselt werden, mit dem der eigentliche Medienstrom verschlüsselt wurde. Solche Verschlüsselungstechniken werden heute noch nicht überall angewendet.

Das „Scrambling“ von einigen älteren Pay-TV-Kanälen basiert meist auf deutlich schwächeren Schutzmechanismen und kann nicht unbedingt als Verschlüsselung bezeichnet werden. Häufig werden die Daten nur „verschleiert“, was ernsthaften Angriffen nicht standhält.

Verschlüsselung von Datenträgern

Eine Möglichkeit, Inhalte, die auf einem Datenträger verteilt werden, zu schützen, besteht darin, die Daten auf dem Datenträger zu verschlüsseln und in einer separaten, ausforschungssicheren Hardware zu entschlüsseln (z.B. eine Chipkarte, die jedem Datenträger beiliegt, ähnlich einem Dongle, mit dem teure Software gegen Raubkopieren geschützt wird). Wie aufwendig der Nachbau eines solchen Hardware-Moduls ist, hängt vom Aufwand ab, mit dem die innere Struktur und die kryptographischen Geheimnisse, die ein solcher Baustein beherbergt, vor Reverse Engeneering (siehe Abschnitt 3.4) geschützt sind. Anhaltspunkte für entsprechende Sicherheitsstufen von Hardwarebausteinen finden sich in Abschnitt 3.2.

Das Abspielgerät besitzt einen Schacht für den Datenträger und einen für die Chipkarte. Eine digitale Kopie der verschlüsselten CD wäre damit ohne die zugehörige Chipkarte wertlos. Allerdings dürfen die entschlüsselten Daten im Abspielgerät nicht unberechtigt abgegriffen werden können, um aus ihnen eine unverschlüsselte digitale 1:1-Kopie herstellen zu können, was aber mit einem PC leicht möglich sein wird. Deshalb ist ein solches Verfahren in der Praxis untauglich und zudem teuer, weshalb es praktisch nicht angewendet wird.

Außerdem verhindert die reine Verschlüsselung der Inhalte auf dem Datenträger nicht das 1:1-Kopieren des (verschlüsselten) Mediums. Deshalb enthält das geschützte Medium neben den verschlüsselten Daten in der Regel noch ein Sondersignal, welches von allgemein zugänglichen Abspielgeräten für den Einsatz in Universalcomputern (PCs) zwar gelesen, aber nicht geschrieben werden kann. Das kann im Prinzip ein einzelnes Datenbit an einer ausgewählten, für Schreibsoftware unzugänglichen Stelle im Datenstrom sein, oder aber, falls Kompatibilität zu existierenden Medien eine Anforderung ist, ein ausgefeilterer Datenkanal, wie etwa bestimmte Kombinationen von Bitfehlern. Abspielgeräte entschlüsseln den Datenstrom nur, nachdem die Anwesenheit des Sondersignals festgestellt wurde. Eine etwas verfeinerte, aber prinzipiell äquivalente Form dieses Prinzips (in der eine Hierarchie aus Schlüsseln teil des Sondersignals ist) findet beispielsweise beim DVD-System Einsatz.

Die Verwendung eines einzigen oder einiger weniger Schlüssel hat den gravierenden Nachteil, dass viele Stellen (z.B. alle Hersteller von Player-Hardware) den Schlüssel erfahren müssen, um ihn in das Endgerät zu integrieren. Sobald eine Stelle „undicht“ wird (oder die Hardware unsicher), ist das gesamte Sicherheitssystem gefährdet. Dies ist beispielsweise beim Content Scrambling System (CSS) der DVD geschehen.

Mehrschlüsselsysteme für Online-Übertragung und Datenträger

Statt einen einzelnen Schlüssel zu benutzen, kann das Risiko etwas reduziert werden, indem eine Gruppe von Schlüsseln benutzt wird, von denen jedes Abspielgerät nur einen beherbergt, z.B. zwei Schlüssel pro Hersteller wie im DVD-System. Der Nutzdatenstrom wird mit einem für die jeweiligen Daten spezifischen Medienschlüssel verschlüsselt, und dieser Medienschlüssel wiederum wird mit allen Schlüsseln aus Abspielgeräten verschlüsselt, wovon jedes Abspielgerät nur einen beherbergt.

Im Prinzip könnten damit, sobald ein Schlüssel aus einem Abspielgerät erfolgreich ausgelesen wurde, die Hersteller von neuen Medien den betreffenden Medienschlüssel nicht mehr mit dem Schlüssel des kompromittierten Abspielgerätes verschlüsselt abspeichern. Dies hätte zur Folge,

dass die entwendete Schlüsselinformation nicht mehr genutzt werden kann, um von neu publizierten Medien den Kopierschutz zu entfernen. Auf der anderen Seite wären aber von dieser Maßnahme die Besitzer aller Abspielgeräte betroffen, die den gleichen nunmehr kompromittierten und aus dem Verkehr gezogenen Schlüssel benutzen. Zudem können mit dem kompromittierten Schlüssel immer noch alle älteren veröffentlichten Werke „entschützt“ werden, was immer noch einen erheblichen Schaden darstellen kann, solange die geschützten Daten nicht nur im Wesentlichen kurzzeitig von Wert sind (wie etwa bei Zeitungsnachrichten).

Mehrschlüsselsysteme werden inzwischen recht erfolgreich im Bereich der digitalen Pay-TV-Zugangskontrolle von mindestens einem Anbieter eingesetzt. Bei Pay-TV-Systemen werden die verteilten verschlüsselten Daten nicht von den Benutzern gespeichert, weshalb ein Austausch von Schlüsseln in dieser Anwendung wesentlich praktikabler ist. Die entsprechenden Systeme sind darauf vorbereitet, dass die Schlüsseldaten in einer Chipkarte untergebracht sind. Chipkarten sind ein Format, das sich insbesondere zum einfachen Postversand eignet. Bei modernen Pay-TV-Systemen besteht daher im Vergleich zu älteren Kopierschutzsystemen, die direkt in die Set-Top-Box integriert sind, kaum ein Bedarf für einen manipulationssicheren Baustein innerhalb der Set-Top-Box: Die Entschlüsselung wird direkt auf der Chipkarte durchgeführt. Der regelmäßige Austausch aller Kundenchipkarten ist im Pay-TV- wie auch im Bank-Bereich inzwischen ein Routinevorgang und bewirkt, dass Geheimschlüssel nach 1–3 Jahren ihren Wert verlieren, was bei Schutzkonzepten für gespeicherte Werke (z.B. DVD) nicht praktikabel ist.

Zusammenfassung

Der Sinn der Verschlüsselung der Nutzdaten ist es, dem Benutzer der Daten den freien Zugriff auf das unverschlüsselte, aber noch komprimierte und damit bequem transportierbare und mit beliebiger Hardware wiedergebbare Nutzsignal vorzuenthalten. Zu diesem Zweck müssen die Schaltfunktionen für

(a) die Erkennung des nicht kopierbaren Sondersignals bzw. der Authentisierung,

(b) die Entschlüsselung,

(c) die Dekompression, und vorzugsweise

(d) auch die Digital/Analog-Wandlung

sowie nach Möglichkeit sogar die physikalische Ausgabe in einer manipulationssicheren geschlossenen Einheit stattfinden, welche den externen Zugang zu Zwischenbearbeitungsschritten verhindert.

2.2.3 Manipulationssichere Hardware

Manipulationssichere Hardware wird zum Schutz von Geheimnissen, etwa Dekodierschlüsseln, und zur Authentisierung der Teilnehmer eingesetzt. Nach einer allgemeinen Problembeschreibung wird das Angreifermodell entwickelt. Schließlich werden die Grundverfahren zur Realisierung manipulationssicherer Hardware beschrieben.

Allgemeines

Die soeben beschriebenen Mechanismen verwenden (meist kryptographische) Geheimnisse, deren Kenntnis die Voraussetzung für die Nutzung der Inhalte ist. Um die Geheimnisse, die gewissermaßen den Anker der Sicherheit der Verfahren bedeuten, vor unberechtigter Verwendung und/oder Kenntnisnahme und womöglich Veröffentlichung zu schützen, müssen sie speziell gesichert werden.

Jedes Abspielgerät enthält dann versteckt innerhalb eines integrierten Schaltkreises die Schlüsselinformation, mit deren Hilfe der Nutzdatenstrom entschlüsselt werden kann. Die Entschlüsselung, digitale Decodierung und Digital/Analog-Wandlung des Nutzsignals sollte innerhalb eines einzigen manipulationssicher geschlossenen Bauteils stattfinden, so dass es extrem schwierig wird, an den entschlüsselten, aber noch digital komprimierten Datenstrom zu gelangen, welcher zum Anfertigen einer exakt identischen Kopie notwendig wäre.

Das Problem dieser Verschlüsselungstechniken ist die sichere Speicherung des Schlüssels (und ggf. auch des gesamten Verschlüsselungsverfahrens) in einem Abspielgerät. Sofern nicht jedes einzelne verkaufte Medium individuell für ein spezielles Abspielgerät verschlüsselt wird, was im Musikbereich mit der existierenden „Plattenladen“-Infrastruktur nicht praktikabel ist, aber für Onlineverkäufe durchaus vorstellbar wäre, so muss es letztendlich einen globalen Schlüssel geben, der in jedem Abspielgerät enthalten sein muss. Gelingt es jemandem, diesen Schlüssel aus einem Abspielgerät auszulesen, so bricht der gesamte Kopierschutz zusammen, da sich nun relativ leicht Software entwickeln lässt, die die Nutzdaten entschlüsselt und damit den Kopierschutz spurenlos entfernt. Dies ist beispielsweise im Spätsommer 1999 für den DVD-Kopierschutz geschehen, und das notwendige Wissen hat sich völlig unkontrollierbar in wenigen Tagen weltweit unter tausenden von technisch Versierten verbreitet. Es gab intensive rechtliche Bemühungen der DVD-Industrie, die Verbreitung eines in den Medien weithin diskutierten DVD-Entschlüsselungsprogramms („DeCSS“) zu unterdrücken, aber inzwischen existiert eine große Anzahl von unabhängigen Implementierungen dieses Entschlüsselungsverfahrens, einige davon weitgehend unbemerkt als Bestandteil normaler MPEG-Abspielsoftware.

Stärke des Angreifers

Die Sicherheit jeder kryptographischen Anwendung basiert letztendlich auf der physischen Sicherung der geheimen Schlüssel gegen den Zugriff durch Unbefugte. Da verteilte Computersicherheitsmechanismen in der Regel mit kryptographischen Techniken (z.B. Verschlüsselungs- und Signaturalgorithmen) realisiert werden, ist die Aufgabe eines manipulationssicheren Systems in der Regel, geheime Schlüssel zu schützen. Neben den eigentlichen Schlüsseln darf für den Angreifer natürlich auch die Ausführung der kryptographischen Algorithmen nicht beobachtbar sein, da aus dem Ablauf des Algorithmus die Schlüssel offensichtlich wären. Neben diesen primär zu schützenden Daten und Algorithmen kann ein manipulationssicheres System noch weitere Anwendungssoftware und andere Komponenten enthalten, die für die Sicherheit des Gesamtsystems relevant sind.

Die historisch ersten praktischen Überlegungen zum Schutz von geheimen Schlüsseln stammen – wie nicht anders zu erwarten – aus dem militärischen Bereich [31]. So wurden beispielsweise auf Kriegsschiffen die Codebücher zur Chiffrierung geheimer Funkmeldungen mit Gewichten versehen und mit wasserlöslicher Farbe gedruckt, so dass die streng geheimen Informationen bei

einem Überfall durch einfaches Überbordwerfen der Bücher schnell und zuverlässig vernichtet werden konnten. Andere Codebücher wurden auf Papier aus Nitrocellulose (Schießbaumwolle) gedruckt, damit sie im Notfall sekundenschnell rückstandsfrei verbrannt werden konnten. Spätere Beispiele von technisch sehr ausgefeilten manipulationssicheren Systemen aus dem militärischen Bereich sind die Sicherheitsmechanismen in Kernwaffen, die nach einem Diebstahl durch Terroristen das spaltbare Material unbrauchbar machen müssen sowie Sensoren, die zur Überprüfung von Abrüstungs- und Kernwaffenteststopp-Verträgen in anderen Ländern installiert werden [2]. Erst etwa 1985 begannen kommerzielle Computerhersteller (angefangen mit IBM) sich außerhalb militärischer Anwendungen mit Konzepten für manipulationssichere Hardware zu befassen. Die Anforderungen im zivilen Bereich unterscheiden sich dabei erheblich von den in Militärausrüstungen gängigen Verfahren. Kosten spielen eine entscheidende Rolle und pyrotechnische Selbstzerstörungsmechanismen sind im Unterhaltungselektronikbereich nicht akzeptabel.

Bislang werden in kommerziellen Anwendungen im Wesentlichen zwei Ansätze zum Entwurf manipulationssicherer Rechner eingesetzt, die im Folgenden näher erläutert sind.

Einchip-Systeme

Sofern die zu schützende Software nur wenige zehntausend Bytes lang ist, kann sie in nichtflüchtigem Speicher zusammen mit der CPU in einem einzigen Mikrocontroller-Chip untergebracht werden. Masken-ROM ist die kompakteste Speicherform auf einem Chip, aber da die Information durch das Chiplayout festgelegt ist, lässt sich ein ROM mit einem Elektronenmikroskop relativ problemlos auslesen. Selbst wenn die ROM-Bits sich nur durch die Dotierungsmuster unterscheiden lassen, stehen geeignete selektive Ätzverfahren zur Verfügung, um diese sichtbar werden zu lassen [37]. Zudem lassen sich Schlüsseldaten im ROM nicht nachträglich ändern oder löschen. Als nicht-flüchtige Speicher in Einchip-Systemen haben sich vor allem EEPROMs durchgesetzt. Dabei handelt es sich um Feldeffekttransistoren, deren Gate-Eingang völlig von isolierendem Material umgeben ist. Durch eine hohe Programmierspannung kann diesem *floating gate* ein bestimmtes Potential aufgezwungen werden, das dann den Schaltzustand des Transistors über viele Jahre hinweg bestimmt, womit ein Bit abgespeichert wird.

Eine sehr weit verbreitete Anwendungsform von EEPROM-Einchip-Systemen sind Chipkarten [30]. Dabei wird der Mikrocontrollerchip auf ein etwa 1 cm^2 großes dünnes Kunststoffplättchen geklebt, das auf der gegenüberliegenden Seite über meist sechs oder acht Kontaktflächen verfügt. Der Siliziumchip wird mit sehr dünnen Gold- oder Aluminium-Bondingdrähten wie in einem normalen Chipgehäuse mit den Kontaktflächen elektrisch verbunden und anschließend in Epoxid-Harz vergossen. Dieses Chipmodul wird zur besseren Handhabbarkeit in eine größere Kunststoffform integriert, zum Beispiel im ISO-Kreditkartenformat, im Miniaturkartenformat wie es bei GSM-Mobiltelefonen eingesetzt wird, oder in einer Plastikschlüsselform, wie sie bei einigen Pay-TV-Decodern zu finden ist.

Zu den Schwächen und Angriffsmöglichkeiten von Einchip-Systemen finden sich im Abschnitt 3.2 auf Seite 50 weitere Informationen.

Sichere Verpackung ganzer Baugruppen

Das grundlegende Problem von EEPROM-basierten Sicherheitsmodulen besteht darin, dass externe Energie benötigt wird, um die geheimen Daten vernichten zu können. Sobald der Angreifer diese Energiezufuhr unterbricht, sind die Daten gefangen und der Zugriff auf die Daten kann in aller Ruhe durchgeführt werden, ohne dass das Auslösen eines Alarmsystems befürchtet werden muss.

Eine attraktive Lösung besteht darin, die geheimen Daten in batteriegepuffertem statischem RAM (SRAM) unterzubringen. Da nun bereits eine Energiequelle erforderlich ist, um die Daten zu erhalten, kann die selbe Energiequelle auch zum Betrieb von wirkungsvollen Alarmmechanismen genutzt werden, die im Fall eines Eindringens in die Schutzhülle des Sicherheitsmoduls einfach die Stromversorgung des SRAM-Speichers unterbrechen. Der Angreifer kann nicht mehr ohne weiteres die Energiequelle entfernen, ohne dadurch die Daten zu gefährden. CMOS SRAM-Bausteine mit 128 Kilobyte Kapazität sind heute mit Erhaltungsströmen von unter 1 µA erhältlich, was eine kleine Lithiumbatterie problemlos mindestens ein Jahrzehnt zur Verfügung stellen kann.

In [56] wurde erstmals der Entwurf eines SRAM-Sicherheitsmoduls dokumentiert, in dem eine ganze Baugruppe mit einem Prozessor, mehreren Speicher- und Peripheriechips, einer kleinen Alarmschaltung und einer Batterie untergebracht ist. Diese Baugruppe wird auf allen Seiten völlig lückenlos und in mehreren Lagen mit einem 80 µm dünnen isolierten Draht umwickelt. Anschließend wird die so umwickelte Baugruppe in ein hartes Epoxid-Harz eingegossen. In diesem Kunststoff befinden sich Aluminium- und Siliziumflocken. Sie sollen die maschinelle Bearbeitung der Verpackung oder deren Entfernung durch einen UV-Laser ohne Beschädigung der Drahtumwicklung oder deren Isolation wesentlich erschweren. Die Isolation des Wickeldrahtes ist chemisch weniger widerstandsfähig als das Vergussmaterial, so dass bei einem Aufätzversuch mit großer Wahrscheinlichkeit Kurzschlüsse entstehen werden. Eine Schaltung aus Operationsverstärkern vergleicht ständig die Widerstände der beiden langen Drahtschleifen, die um die Baugruppe gewunden wurden. Wenn sich durch eine Unterbrechung oder einen Kurzschluss die Widerstandsverhältnisse deutlich ändern, so wird sofort die Spannungsversorgung der SRAM-Chips mit Masse kurzgeschlossen, so dass die Daten gelöscht werden. Diese Schaltung benötigt nur etwa 20 µA Strom.

Zu den Schwächen und Angriffsmöglichkeiten auf sicher verpackte Baugruppen finden sich im Abschnitt 3.2 auf Seite 52 weitere Informationen.

2.2.4 Sandbox-Verfahren

Sandbox-Verfahren dienen dem Schutz der Ausführungsumgebung und anderer Programme vor bösartigem Programmcode, der meist erst online und zur Laufzeit des Systems bekannt wird. Der Programmcode läuft deshalb zum Schutz innerhalb eines abgesicherten Bereiches – der Sandbox. Sandbox-Verfahren sind heute in allen gängigen Web-Browsern vorinstalliert und dienen zum Schutz des Surfers bzw. seines Rechners vor möglicherweise bösartigen Java-Applets. Allgemeiner formuliert, schützt die Sandbox vor bösartigen Inhalten. Sie muss also bereits auf der Plattform des Nutzers installiert sein und kann nicht erst duch die Inhalte selber bereitgestellt werden.

Die Ausführung fremder Softwareprogramme ist, sofern sie völlig ohne Einschränkungen ausgeführt werden, mit Risiken für die Ausführungsumgebung und andere in der Ausführungsumgebung laufende Programme verbunden. Beispielsweise könnte fehlerhafter oder absichtlich bösartiger Programmcode (malicious code), der von einem Web-Browser geladen und direkt auf dem Betriebssystem zur Ausführung gebracht wird (sog. aktiver Inhalt, beispielsweise ActiveX-Control), mit allen Rechten der Ausführungsumgebung (hier: Web-Browser) arbeiten, d.h. beliebige Dateien lesen, anlegen, meist auch löschen oder verändern. Weiterhin ist es nicht ausgeschlossen, dass ungewollte Interaktionen mit anderen momentan laufenden Programmen stattfinden. So könnte beispielsweise ein legal und kostenpflichtig bezogener Medienstrom unbemerkt vom malicious code „abgezweigt“ und ins Internet eingespeist werden, oder der malicous code kopiert sich die Zugangsdaten, um den Stream anschließend unberechtigt anzufordern.

Die Anforderung, dass eine Ausführungsumgebung sich selbst und die laufenden Anwendungen schützen muss, ist nicht neu. Jedes Betriebssystem ist gewissermaßen eine Ausführungsumgebung und muss selbst über Schutzmechanismen verfügen, etwa die Vergabe von Zugriffsrechten (z.B. Leserecht, Schreibrecht, Ausführungsrecht) und den Speicherschutz, d.h. Programme erhalten vom Betriebssystem zugeteilten Speicher und dürfen nur diesen verändern, andernfalls wird eine Speicherschutzverletzung gemeldet.

Die Schutzmechanismen des Betriebssystems sind jedoch für fremde aktive Inhalte, die möglicherweise erst zur Laufzeit des Systems geladen werden, viel zu grobkörnig und unflexibel.

So mag eine Pay-TV-Anwendung beispielsweise Zugriff auf eine Conditional-Access-Komponente der Set-Top-Box bekommen, ein über das Internet heruntergeladenes und in der Set-Top-Box als Videospiel ausgeführtes Spieleprogramm, das in Wirklichkeit ein trojanisches Pferd ist, mit dem die Encryption Keys des Nutzers unbemerkt ausspioniert werden sollen, darf dagegen keinen Zugriff erlangen. Die Set-Top-Box muss also in Abhängigkeit der Anwendung größtenteils ohne Zutun des Menschen entscheiden, welche Anwendungen welche Rechte erlagen dürfen.

Die Schutzmechanismen des Betriebssystems sind zudem vom Betriebssystem abhängig. Dies widerspricht jedoch dem Trend, aktive Inhalte auf verschiedenen Plattformen betriebssystemunabhängig, aber trotzdem sicher ausführen zu wollen. Deshalb hat man – je nach aktivem Inhalt – Auführungsumgebungen geschaffen, die die Schutzanforderungen betriebssystemunabhängig realisieren.

Sicherheit von Java, Java-Script, ActiveX-Controls und Plug-ins

Im Internet findet man aktive Inhalte in Form von ActiveX-Controls, Java-Applets und Java-Scripts.

Java-Applets werden durch die Ausführungsumgebung – meist als Java Virtual Machine (JVM) bezeichnet – vollständig abgeschottet. Die JVM verfügt über eine ausgefeilte Zugriffskontrolle. So besitzen Java-Applets standardmäßig keinerlei Lese- und Schreibrechte auf dem Rechner, auf dem sie ausgeführt werden. In diesem Sinn wird auch der Begriff Sandbox verwendet, da ein Java-Applet innerhalb des Sandkastens – jedes Applet hat seinen eigenen Sandkasten – beliebige Operationen ausführen darf, aber ihn nicht verlassen kann. Da dies jedoch Einschränkungen bzgl. der realisierbaren Anwendungen mit sich bringen würde (z.B. könnte ein Home-Banking-Applet dann nicht mit der HBCI-Chipkarte kommunizieren), dürfen

Java-Applets, die vom Benutzer als vertrauenswürdig eingestuft wurden, zusätzliche Rechte (Schreib-, Lese-, Ausführungsrechte) anfordern und nach Bestätigung durch den Endbenutzer auch erhalten. Um die Authentizität des Codes (als eine Voraussetzung für die Beurteilung der Vertrauenswürdigkeit des Bereitstellers des Applets) sicherzustellen, können Java-Applets digital signiert sein (code signing). Das Sicherheitsmodell von Java umfasst also eine Public-Key-Infrastruktur (PKI). Die zur Prüfung der Signaturen erforderlichen Zertifikate sind Bestandteil der JVM bzw. der Web-Browser. Da Java eine betriebssystemunabhängige Plattform ist, lassen sich Applets auch auf verschiedenen Rechnern, Devices und Betriebssystemen ausführen, sofern sie die Java-Plattform unterstützen.

Java-Scripts werden im Web-Browser ausgeführt und besitzen aufgrund des geringen Sprachumfangs bei richtig implementiertem und konfiguriertem Browser nahezu keine Möglichkeiten, ernsthaften Schaden anzurichten. In der Vergangenheit wurden allerdings wiederholt Sicherheitslöcher entdeckt, die meist auf Implementierungsfehler im Web-Browser zurückgingen. Beispielsweise bietet Georgi Guninski auf seiner Webseite http://www.guninski.com/ Sicherheitshinweise und Demonstrationen der Schwächen für alle gängigen Browser-Typen an.

ActiveX ist eine von Microsoft entwickelte proprietäre Schnittstellenbeschreibung zur Ausführung von betriebssystemabhängigem Programmcode. ActiveX-Controls werden nur sehr rudimentär in ihren Ausführungsrechten eingeschränkt. Im wesentlichen erhalten sie die betriebssystemabhängig vergebenen Rechte und sind insofern sehr gefährlich, da sie meist ohne Einschränkungen laufen. Der Chaos Computer Club konnte z.B. nachweisen, dass ein bösartiges ActiveX-Control selbständig Homebanking-Funktionen auslösen kann [15].

Multimedia Home Platform

Die Vorteile der Java-Plattform mit ihrer flexiblen Anwendungsgestaltung sollen künftig auch im Bereich interaktive Dienste und digitales Fernsehen genutzt werden. Mit der Multimedia Home Platform (MHP) wurde durch ETSI (European Telecommunications Standards Institute) ein offener Standard für das digitale Fernsehen der Zukunft geschaffen [16].

Mit MHP werden Personal Computer und TV mehr und mehr miteinander verschmelzen. Für den Verbraucher hat MHP den Vorteil, über eine Plattform, d.h. konkret über ein einziges Gerät viele Medien, Dienste und Programme empfangen zu können. Das Gerät wird meist eine Set-Top-Box sein, aber auch der Multimedia-PC ist als Endgerät denkbar.

Das Ziel von MHP ist u.a. die Realisierung von interaktivem Fersehen. MHP unterscheidet drei Profile der Interaktivität:

- Enhanced broadcasting, bei dem kein Rückkanal existiert,
- Interactive broadcasting mit Rückkanal sowie
- Internet access.

Bei den beiden Broadcasting-Profilen werden neben dem Fernsehbild (MPEG-Stream) noch zusätzliche Daten, z.B. sogenannte Xlets, übertragen. Ein Xlet ist im wesentlichen eine spezielle Form von Java-Applet, das in einer Ausführungsumgebung innerhalb einer Sandbox ausgeführt wird. Die Xlets werden dabei über ein „Objektkarussell“ ausgestrahlt, ähnlich dem heutigen Videotext. Die wesentlichen Unterschiede zwischen Xlets und Java-Applets bestehen in

- der Nutzbarkeit speziell für das Fernsehen konzipierter graphischer Bedienelemente, die Halbtransparenz unterstützen, z.B. Textfelder und Knöpfe, die das darunter liegende Fernsehbild nicht völlig verdecken,
- einem reduzierten Umfang an Java-Programmierbibliotheken, um MHP-fähige Geräte nicht unnötig zu verteuern,
- Synchronisationsfunktionen mit MPEG-Stream und Funktionen zu seiner Steuerung und ggf. weiteren Multimediadaten (z.B. Einblendungen)
- einer Conditional-Access-Schnittstelle, die für die Anbindung verschiedener Entschlüsselungssysteme von Pay-TV-Inhalten vorgesehen ist, sodass der Kunde auch tatsächlich viele Kanäle (auch unterschiedlicher Anbieter) mit einem einzigen Gerät empfangen kann.

MHP ist ein offener Standard, der problemlos auch auf einem PC implementiert werden kann. Die Offenheit des Standards legt es nahe, auch Implementierungen mit offengelegten Quelltexten von MHP zuzulassen und zu fördern. Dies würde zur Vermeidung von Programmierfehlern beitragen. In [18] wird beispielsweise der Vorschlag einer Open-Source-Implementierung von MHP gemacht.

Set-Top-Boxen, die MHP implementieren, werden teilweise auf Standardbetriebssystemen implementiert. Neben Windows-Betriebssystemen werden auch Linux sowie spezielle eingebettete Systeme verwendet.

Das Sicherheitsmodell von MHP ist dem von Java sehr ähnlich. Xlets können digital signiert sein und dürfen sich um weitere Rechte bewerben. Unsignierte Xlets dagegen haben nicht auf den vollen Funktionsumfang von MHP Zugriff.

Das insgesamt gut durchdachte Sicherheitsmodell von MHP enthält leider eine Funktionalität, die in der Praxis sehr gefährlich werden kann und die praktische Sicherheit stark reduziert: Das ansonsten konsequent angewendete Sandbox-Prinzip wird durchbrochen durch eine sog. Plug-in-Architektur, die es erlaubt, den Funktionsumfang (bzgl. dekodierbarer Formate) der Set-Top-Box zu erweitern [16, S.35f]. Plug-ins sollen sich jedoch ebenfalls authentisieren, um erweiterten Zugriff auf MHP-Komponenten zu bekommen. Genauere Informationen hierzu enthält der MHP-Standard nicht, man kann jedoch davon ausgehen, dass die Sicherheitsrisiken im schlimmsten Fall denen der Anwendung von Browser-Plug-ins oder ActiveX entsprechen und somit im Einzelfall ein ernstes Sicherheitsproblem darstellen können.

2.3 Spezielle DRM-Techniken

Neben den grundsätzlichen Sicherheitsmechanismen entstanden auf die Schutzziele von DRM-Systemen abgestimmte Sicherheitsmechanismen. Im Folgenden werden

- Modifikation des analogen Endsignals,
- Watermarking und
- Fingerprinting

behandelt.

2.3.1 Modifikation des analogen Endsignals

Selbst wenn die Entschlüsselung, Dekompression und Analogwandlung des Audio- oder Videosignals in einer manipulationssicher geschlossenen Einheit stattfindet, so steht dem Kopierer immer noch ein hochwertiges Analogsignal zur Verfügung, das sich wiederum Digitalisieren und Komprimieren lässt. Dieser Vorgang muss nur ein einziges Mal durchgeführt werden. Alle weiteren Kopien können völlig ungeschützt und digital vorgenommen werden. Das qualitativ hochwertige Anzapfen und Wandeln eines Analogsignals erfordert gewisse technische Sorgfalt, insbesondere wenn das Analogsignal bewusst nicht in einer gängigen Form zur Verfügung steht.

Allerdings sind entsprechende Adapterschaltungen von jedem elektronisch geschulten Techniker vergleichsweise leicht aus Standardkomponenten herzustellen. Immerhin wäre es möglich, wenigstens die Rückwandlung des Analogsignals durch Laien zu verhindern, indem keine externen Steckverbinder mit Analogsignalen vorgesehen werden und die Entschlüsselung und Analogwandlung in der Nähe von schwer zugänglichen Komponenten, etwa dem Hochspannungsteil eines Videomonitors oder in einem in den Lautsprecher oder Kopfhörer integrierten Baustein, durchgeführt wird. Viele Kunden werden aber durch die resultierende Inkompatibilität mit anderer Unterhaltungselektronik enttäuscht sein, da diese Einschränkungen der systemintegrierenden Grundidee des Multimedia-Gedanken zuwiderlaufen.

Im Falle von Flachbildschirmen als Wiedergabemedium ist es jedoch technisch praktikabel, die Entschlüsselung und die Bildausgabe so eng miteinander zu verbinden, dass sich selbst technische Experten einem erheblichen Aufwand gegenüber sehen, da Flachbildschirme mit hochgradig parallelen Ansteuersignalen arbeiten, es also im Gerät bei sorgfältig integrierter Entschlüsselungsfunktion keine einfach anzapfbare Analogform des Bildsignals gibt, wie dies bei Kathodenstrahlröhren der Fall ist.

Modifikationen des analogen Endsignals können auch dem Zwecke dienen, eine „Entdekomprimierung“ zu erschweren. Wärend bei einer normalen Komprimierung von audiovisuellen Daten immer Information verloren geht, besteht bei manchen Kompressionsverfahren die Möglichkeit, mit dem Wissen, dass ein analoges Signal durch einen exakt bekannten Dekompressionsalgorithmus aus unbekannten komprimierten Daten entstanden ist, diese komprimierte Form nahezu exakt zu rekonstruieren. Dadurch kann eine sorgfältige „Entdekomprimierung“ mit einer wesentlich geringeren Qualitätseinbuße verbunden sein als die erneute Anwendung des ursprünglichen Kompressionsalgorithmus. Die genauen Möglichkeiten und Grenzen der Entdekomprimierung sind bislang noch nicht hinreichend untersucht worden, aber neben der noch ausstehenden gezielten Entwicklung von Dekompressionsverfahren, die gegen diese Technik geschützt sind, besteht auch die Möglichkeit, durch Filterung und Addition eines kleinen Rauschsignals Entdekompressionsversuche zu erschweren.

Macrovision

Ein weiteres Beispiel für eine Modifikation des analogen Endsignals ist das Video-Kopierschutzsystem der kalifornischen Firma Macrovision [42, 46]. Dieses System nutzt die Tatsache aus, dass die Elektronik am Videoeingang von Fernsehern und VHS-Videorekordern unterschiedlich auf analoge Videosignale reagiert, welche die Fernsehnorm verletzen. Im Gegensatz zu Fernsehempfängern verfügen VHS-Videorekorder über eine automatische Pegelsteuerung, die in der Lage ist, Spannungsschwankungen im Eingangssignal automatisch auszuglei-

chen. Vorbespielte Videokassetten, die unter Verwendung des Macrovision-Kopierschutzes hergestellt wurden, enthalten in der Austastlücke (einem Teil des Bildsignals, der auf normalen Fernsehgeräten nicht sichtbar ist) Bereiche, in denen Spannungen außerhalb des normalen Helligkeitsbereiches auftauchen. Die automatische Pegelkontrolle in einem aufzeichnenden VHS-Heimrekorder reagiert auf diese Überspannungen durch Herunterregeln der Verstärkung, wodurch das beim Kopieren vom Rekorder aufgenommene Bild insgesamt dunkler wird. Da die Überspannungen ständig wechseln, springt die Helligkeit des aufgezeichneten Videosignals, was zu einer erheblich verschlechterten Widergabequalität des kopierten Videos führt.

Die Pegelsteuerung des Videosignals ist nicht zwingend erforderlich und nur sehr wenige Techniken zur Pegelsteuerung lassen sich durch das Macrovision-Verfahren so stark irritieren, dass es zu Problemen bei der Bildaufzeichnung kommt. Aus diesem Grund hat die japanische Firma JVC, die Lizenzgeberin für das heute dominierende analoge Heimvideoformat VHS ist, vor einiger Zeit die Lizenzbedingungen für Hersteller so geändert, dass eine bestimmte für Macrovision besonders empfindliche Pegelsteuertechnik für alle VHS-Videorekorder zwingend vorgeschrieben ist.

Der Macrovision Kopierschutz lässt sich technisch vergleichsweise einfach auf verschiedene Arten umgehen. Eine Möglichkeit ist die Deaktivierung der Pegelsteuerung im aufzeichnenden Videorekorder, was insbesondere bei älteren Geräten oft durch Austausch eines einzigen elektronischen Bauteils möglich ist. Eine weitere Möglichkeit sind externe Filterschaltkreise die zwischen den wiedergebenden und aufnehmenden Rekorder geschaltet werden. Sie lassen die sichtbaren Bildbestandteile eines Videosignals ungehindert passieren, aber die Synchronisationspulse und anderen Signale in der Austastlücke werden neu und somit frei von Überspannungen erzeugt. Die meisten Elektroniker mit guten Videotechnikkenntnissen werden kaum mehr als eine Woche benötigen, um durch Beobachtung des Videosignals mit einem Oszilloskop das Macrovision-Prinzip zu verstehen und eine einfache Version einer derartigen Kopierfilterschaltung zu entwickeln, die mit Hilfe von elektronischen Bauelementen realisiert werden kann. Solche Bauelemente finden auch in jedem Fernsehgerät Verwendung, sind in Bastelläden erhältlich und kosten insgesamt weniger als 50 EUR. Zahlreiche Beschreibungen von Macrovision-Filterschaltungen in Elektronikmagazinen und Internet-Seiten belegen dies.

Derartige Filterschaltungen waren auch einige Zeit kommerziell verfügbar, allerdings hat die Firma Macrovision sorgfällig fast jede denkbare Bauform schon vor Einführung des Systems patentieren lassen, und konnte somit den kommerziellen Vertrieb dieser Produkte recht erfolgreich mit rechtlichen Mitteln einschränken. Allerdings existiert eine Reihe von völlig legitimen Videotechnik-Produkten, die nicht speziell als Macrovision Kopierschutzfilter entwickelt wurden, die aber dennoch die Synchronpulse regenerieren und somit ganz nebenbei auch den Macrovision-Schutz vollständig entfernen. Dazu gehören zum Beispiel verschiedene Videoschnitt-Graphikkarten für PCs, professionelle Videoausrüstung zum Verbessern der Signalqualität in Videostudios (*time base correctors*), sowie verschiedene Videoeffekt-Geräte und Videorekorder, die nicht mit dem VHS-Standard arbeiten. Auch wenn das Macrovision System eine gewisse Hemmschwelle für den elektronisch unversierten Endkunden darstellt und verhindert, dass nur mittels einfachen Verbindens zweier Heimrekorder gute Kopien erstellt werden könnten, so lässt sich die Technik doch mit etwas Sachverstand und einer geringfügigen Investition mühelos umgehen.

Macrovision wird heute nicht nur in vorbespielten Videokassetten zum Verleih oder Verkauf eingesetzt, sondern auch in DVD-Abspielgeräten und Pay-TV-Zugriffskontrollsystemen. Bei

diesen findet nach Möglichkeit die Entschlüsselung, Dekompression, digital/analog-Wandelung und das Einfügen der Macrovision-Schutzimpulse in einem einzigen manipulationssicher gekapselten integrierten Baustein statt. Die Vertriebsfirma fügt dem komprimierten digitalen Videosignal vor der Verschlüsselung Steuerinformationen bei, die im Abspielgerät nach der Dekompression die Hinzufügung der Fernsehnorm-verletzenden Überspannungen auslösen. Somit lässt sich die Anfertigung von analogen Kopien mit einem Heimrekorder auch vom Analogausgang eines DVD-Players oder einer pay-per-view Set-Top-Box für ausgewähltes Material erschweren.

2.3.2 Watermarking zur Detektion von übertragenen Inhalten und zum Schutz vor Verfälschung

Beim Watermarking werden in digitale Mediendaten Informationen z.B. über den Urheber der Daten eingebettet. Die mit dem Original fest verbundene, eingebettete Information wird als Watermark bezeichnet (Abbildung 2.4). Dieser Einbettungsprozess muss so robust erfolgen, dass es unmöglich ist, das Watermark unberechtigt zu entfernen, wenn der Angreifer versucht, das Objekt zu manipulieren. Dabei sind viele verschiedene Manipulationen denkbar: Analog-Digital-Wandlung, Digital-Analog-Wandlung, Ausdrucken und erneutes Einscannen, Verändern von Größe, Auflösung, Abspielgeschwindigkeit, Farbtiefe, Kompression, Verzerrung, Ausschneiden von Bildteilen.

Es ist klar, dass das Watermark möglichst so in das digitale Objekt eingebracht werden muss, dass es nicht zu Beeinträchtigungen des Dokumentes kommt. So sollten Watermarks in Grafiken bzw. Videos nicht sichtbar, in Sounddateien nicht hörbar sein. Insofern sind die Watermarking-Verfahren verwandt mit der Steganographie [19, 44], wo versucht wird, geheime Daten unbemerkt und damit vertraulich in Hülldaten (z.B. Bilder, Musik) einzubetten.

Gegenwärtige Watermarkingtechniken arbeiten bevorzugt im Frequenzbereich (neben Raum- und Zeitbereich), den die digitalen Objekte abdecken [12, 54, 57]. Dazu werden sog. Spread Spectrum Techniken eingesetzt. Die Einbettung muss dabei auch in die Datenteile erfolgen, die auch nach einer verlustbehafteten Kompression, die nicht wahrnehmbare oder redundante Daten entfernt, noch vorhanden sind.

Die Information, die das Watermark trägt, ist vom Einsatzzweck (Urheberrechts- oder Eigentumsrechtsschutz) und der zur Verfügung stehenden Infrastruktur abhängig. Das kann z.B. eine Dokument-ID sein oder der Name des Autors.

Ein praktisches Anwendungsbeispiel für watermarkierte Ton- und Videodaten ist das automatisierte Erstellen von Distributionsprotokollen beim Webcasting: Ein Scanner, der z.B. von einer Verwertungsgesellschaft betrieben wird, analysiert die gesendeten Daten z.B. eines Webradios nach eingebetteten Watermarks, um anschließend die Rechte des Künstlers wahrnehmen zu können, Hitlisten zu erstellen etc.

Watermarking-Systeme besitzen neben der hier beschriebenen technischen Komponente auch eine organisatorische. Jedes digitale Objekt muss vor der Distribution in einer vertrauenswürdigen Registrierungsstelle gemeldet sein, damit zweifelsfrei nachvollziehbar ist, wer der Urheber eines Inhaltes ist. Da technisch nicht verhinderbar ist, dass ein bereits markierter Inhalt erneut markiert wird, muss der tatsächliche Urheber den Zeitpunkt seiner Markierung nachweisen können. Alternativ zur Registrierung kann auch ein von einer vertrauenswürdigen Stelle

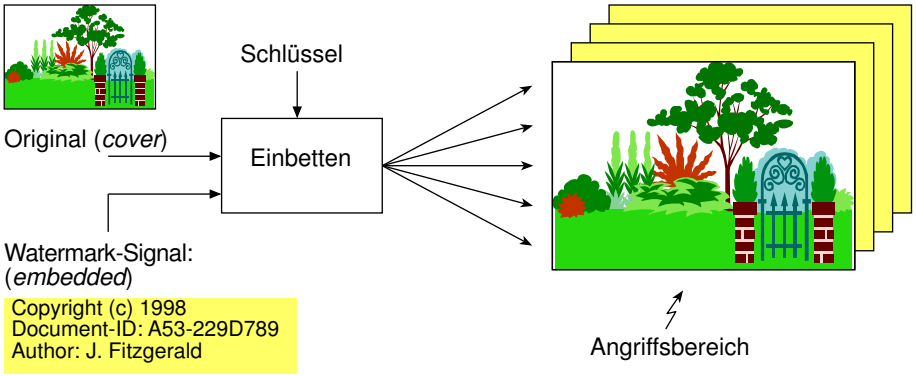

Abbildung 2.4: Distribution eines markierten digitalen Objekts

digital signiertes (und damit authentisches) Datum-Uhrzeit-digitales-Objekt-Kennzeichen Teil der einzubettenden Information sein. Da digitale Signaturen heute mehrere hundert bis einige tausend Bit einnehmen können, ist dies jedoch nicht in jedem Fall realisierbar, und um eine vertrauenswürdige dritte Stelle kommt man ebenfalls nicht herum.

Informationen zum momentan erreichbaren Sicherheitsniveau von Watermarking-Systemen finden sich in Abschnitt 3.3.

2.3.3 Fingerprinting zum Verhindern der nicht verfolgbaren Weitergabe von Inhalten

Sofern das Kopieren von Inhalten nicht verhindert werden kann, möchte man wenigstens abschreckende Maßnahmen ergreifen, die das unberechtigte Kopieren von Inhalten erkennbar und verfolgbar machen.

Kennzeichnung des Inhalts

Beim Fingerprinting werden in digitale Mediendaten Informationen über den Käufer eingebettet. Der Anbieter kennzeichnet jede verkaufte Kopie durch kleine Änderungen so, dass später beim Auffinden einer Raubkopie der ursprüngliche Käufer festgestellt werden kann. Dieses kundenindividuelle Watermarking wird *Fingerprinting* genannt. Fingerprinting-Verfahren werden u.a. in [7, 8, 17, 45, 50] vorgestellt.

Da nun mehrere Repräsentationen der Daten entstehen, die sich jeweils genau durch den Fingerprint unterscheiden, ergibt sich folgende Zusatzforderung: Ein Angreifer soll selbst dann nicht in der Lage sein, den Fingerprint zu entfernen, wenn er im Besitz mehrerer Kopien eines markierten Inhaltes ist (Kollusionsresistenz).

Die Anzahl der notwendigen Kopien zum Entfernen des Fingerprints bzw. zum Bilden eines anderen (entweder eines neuen oder einem anderen Käufer zugeordneten) Fingerprints wird als Kollusionsresistenz bezeichnet. Mit steigender Kollusionsresistenz wächst allerdings auch der Einbettungsaufwand der Verfahren.

Durch sog. asymmetrisches Fingerprinting [50] kann zusätzlich sichergestellt werden, dass der Anbieter des Medienstroms keine gefälschten „Beweise“ erzeugen kann.

Kennzeichnung des Schlüssels

Eine Sonderform des Fingerprinting ist die Schlüsselkennzeichnung. Sie wird angewendet, wenn die Verteilung von individuell markierten Inhalten zu aufwendig oder nicht möglich ist, z.B. auf Datenträgern (CD, DVD) oder beim Broadcasting (z.B. Pay-TV). Alle Kunden erhalten so gleiche digitale Daten.

Um die unberechtigte Nutzung der Inhalte durch Aussenstehende von vorn herein auszuschließen, werden die Inhalte verschlüsselt übertragen. Nun könnte jeder Kunde den Entschlüsselungsschlüssel in einem vor Ausforschung physisch sicheren Gerät (z.B. einer Chipkarte oder einem gekapselten Player) erhalten, um zu verhindern, dass er den Schlüssel unberechtigt weitergibt. Physischer Schutz gelingt jedoch bestenfalls für eine beschränkte Zeit, da immer wieder einmal neue Methoden zum unberechtigten „Auslesen“ von geheimen Informationen z.B. aus Chipkarten gefunden werden.

Besser wäre es also, wenn jeder Kunde einen eigenen individuellen Schlüssel zur Entschlüsselung des Medienstroms bekäme. Ein Verschlüsselungsverfahren, mit dem es möglich ist, einen einzigen verschlüsselten Medienstrom an alle Empfänger zu senden, der dann mit mehreren individuellen Schlüsseln entschlüsselt wird, wird als Gruppenverschlüsselung (auch: Broadcast Encryption) bezeichnet (Abbildung 2.5).

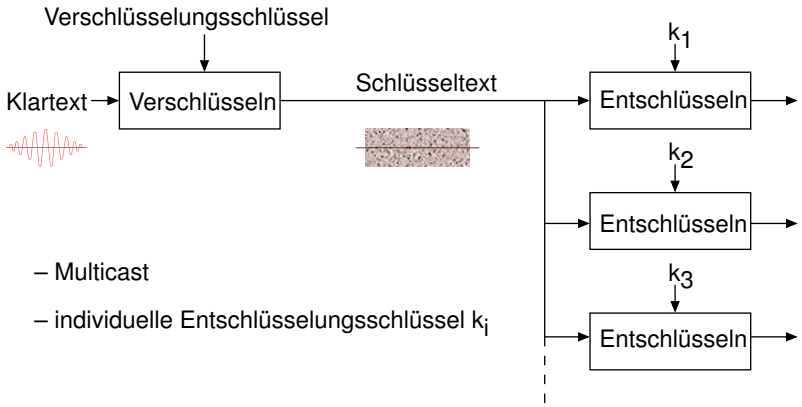

Abbildung 2.5: Gruppenverschlüsselung

Taucht ein Entschlüsselungsschlüssel illegal im Internet auf, kann der legale Besitzer ermittelt und ggf. verantwortlich gemacht werden für die unberechtigte Veröffentlichung des Schlüssels. Dieser Prozess der Rückverfolgung (Traitor Tracing) gelingt jedoch nur, wenn gespeichert wurde, welcher Kunde welchen Schlüssel erhalten hat. Zur Identifizierung des legalen Besitzers wird dann nicht der digitale Inhalt, sondern der Entschlüsselungsschlüssel mit einem Fingerprint versehen.

Zur eigentlichen Entschlüsselung des Medienstroms erhält der Kunde vom Anbieter den Schlüssel und weitere Berechnungsdaten, mit denen er den augenblicklichen Entschlüsselungsschlüssel berechnen kann.

Es muss verhindert werden, dass besonders böswillige Kunden, die sich gleich mehrere Schlüssel legal besorgen, aus ihnen einen neuen Schlüssel berechnen können. In diesem Fall wäre die Rückverfolgung entweder erfolglos (d.h. es wurde ein Schlüssel berechnet, der nicht

registriert ist) oder ein Kunde wird fälschlich beschuldigt (d.h. der berechnete Schlüssel ist identisch mit dem eines anderen Kunden).

Schlüsselmarkierung ist vor allem dort sinnvoll, wo der Wert der Daten im Vergleich zu den Kosten für die Verteilung relativ gering ist: Ein Pirat könnte einen Medienstrom mit einem legal erworbenen Schlüssel entschlüsseln und erneut (illegal und unverschlüsselt) verteilen, da die Inhalte selbst keine Rückschlüsse auf den Piraten zulassen [50].

Konkrete Verfahren für Schlüsselkennzeichnung werden beispielsweise in [10, 25, 48, 49] vorgeschlagen.

Kollusionsresistenz

Insbesondere Fingerprinting-Verfahren aber auch Watermarking-Verfahren (Abschnitt 2.3.2) und zum Teil kryptographische Verfahren generell (Abschnitt 2.2.1) müssen sicher gegen sog. Collusion Attacks sein. Ziel des Angreifers ist es,

- aus mehreren, individuell für verschiedene Konsumenten hergestellten Kopien des gleichen Inhalts diejenigen Stellen des Inhalts zu ermitteln, an denen ein rückverfolgbares Kennzeichen eingebracht wurde, oder
- aus mehreren zur Entschlüsselung desselben Inhalts geeigneten Schlüsseln einen neuen Schlüssel zu berechnen, der dann nicht mehr zurückverfolgbar ist.

Gute Fingerprinting-Verfahren halten in der Regel solchen gemeinschaftlichen Angriffen bis zu einem gewissen Grad (Kollusionsresistenz, Anzahl verfügbarer Kopien) stand. Diese Aussage bezieht sich natürlich nur auf Angriffe, die nicht auf die Watermarking-Eigenschaft jedes Fingerprints gerichtet sind: Fingerprinting kann nie sicherer sein als Watermarking.

Fingerprinting zur Detektion von Inhalten

Neben dem oben erläuterten Begriffsverständnis von Fingerprinting, das auf das *Einbringen* eines Fingerabdrucks des Käufers in den Inhalt zielt, existiert noch ein weiteres: Jeder Inhalt besitzt in sich eine einzigartige Charakteristik, die es möglich macht, ihn zu erkennen und von anderen zu unterscheiden. Dabei geht es weniger um Sicherheitseigenschaften, sondern um das automatisierte Erkennen von Strukturen. Der Inhalt selbst wird dabei nicht verändert.

Seit Jahren forscht man, um die Erkennungsrate und -geschwindigkeit solcher Verfahren zu verbessern. Ein Beispiel für eine solche Detektionstechnik ist AudioID, die am Fraunhofer Institut für Integrierte Schaltkreise (IIS-A) entwickelt wurde (http://golem.de/0201/17862.html). Um ein bekanntes Musikstück eindeutig identifizieren zu können, sollen nur wenige Sekunden Musikmaterial ausreichen. Über sogenannte Spektralflachheitseigenschaften einzelner Frequenzbänder des Musikstücks, die verglichen werden mit einer Datenbank, die die Fingerabdrücke aller detektierbaren Musikstücke enthält, wird das Musikstück erkannt.

Hier zeigt sich ein wesentlicher Unterschied zu Watermarking-Verfahren: Ein in den Inhalt eingebettetes Watermark enthält Daten (beispielsweise den Namen und Interpreten des Musikstücks), die durch den Extraktionsalgorithmus ausgelesen werden können und sofort, d.h. ohne zusätzliche Online-Verbindung zu einer Datenbank, zur Verfügung stehen.

Solche Fingerprinting-Techniken eignen sich beispielsweise zum Erstellen automatisierter Sendelisten von Rundfunk- und Fernsehsendungen. Als Detektionsmittel zum Aufspühren (Abschnitt 2.4.5) illegaler Angebote und anschließenden Filtern (2.4.6) sind sie bedingt geeignet. Auch zur Rückverfolgung (Traitor Tracing) eignen sie sich nicht.

2.4 Schwache Mechanismen

Neben den Kerntechniken, die in den vorangegangenen Abschnitten beschrieben wurden, existieren noch Mechanismen, die auch einen gewissen Schutz der Inhalte gegen unberechtigte Nutzung bieten. Im sicherheitstechnischen Sinn zählen sie aber nicht zu den Mechanismen, die gegen entschlossene, intelligente Angreifer schützen.

Diese „schwachen Mechanismen“ wirken somit bestenfalls unterstützend und vor allem gegen „unbedarfte Angriffsversuche“.

2.4.1 Einbringen von Codes ohne besondere Sicherung

Gerade in der Anfangszeit digitaler Kopierschutztechniken wurden entsprechende Codes in Inhalte eingebracht, die anzeigen sollen, welche Nutzungsrechte mit dem Inhalt verbunden sind. Aus dem Softwarebereich sind solche „Freischaltcodes“ seit langem bekannt. Leider können diese Codes leicht weitergegeben werden und im Internet wimmelt es nur so von Webseiten, die solche Registration Codes enthalten.

Solange diese Codes nicht so fest mit dem Inhalt selbst verbunden sind, dass der Inhalt nur mit dem entsprechenden Code nutzbar ist, sind solche einfachen Systeme leicht zu umgehen, was nachfolgend am Beispiel des Serial Copy Management Systems (SCMS) gezeigt werden soll. Ein ähnlich einfacher Mechanismus, den man ebenfalls unter die hier behandelte Kategorie zählen kann, ist der analoge Kopierschutzmechanismus von Macrovision (siehe Abschnitt 2.3.1).

Beispiel Serial Copy Management System

Eines der ersten digitalen Kopierschutzsysteme ist das Serial Copy Management System (SCMS), das im Jahre 1990 für den digitalen Home-Audio-Bereich auf Initiative der RIAA (Recoding Industry Association of America) eingeführt wurde.

Jeder digitale Audio-Recorder, d.h. momentan CD-R-Audio, MiniDisc (MD), Digital Audio Tape (DAT), der über einen digitalen SPDIF-Ausgang (Sony Philips Digital Interface) verfügt, muss auch SCMS implementieren.

SCMS-geschützte Inhalte enthalten alle 75 Datenblöcke (Frames) ein Kopierschutzbit, das entweder dauerhaft eingeschaltet, ausgeschaltet oder abwechselnd ein- und ausgeschaltet wird. In SCMS können demnach drei Situationen unterschieden werden:

1. **Frei kopierbare Inhalte:** Hier ist das Kopierschutzbit im Original dauerhaft ausgeschaltet, und die Inhalte können ohne Restriktionen kopiert werden. Das Kopierschutzbit der Kopie ist ebenfalls dauerhaft ausgeschaltet, so dass von der Kopie wieder Kopien angefertigt werden können.

2. **Einmal kopierbare Inhalte:** Hier ist das Kopierschutzbit im Original dauerhaft eingeschaltet. Eine von diesem Original angefertigte Kopie verändert das Kopierschutzbit so, dass es abwechselnd ein- und ausgeschaltet ist.

3. **Nicht kopierbare Inhalte:** Empfängt ein mit SCMS ausgestatteter Audio-Recorder Inhalte mit sich wechselndem Kopierschutzbit, verweigert er das Anfertigen einer Kopie.

SCMS kann in der Praxis leicht umgangen werden.

- Da Inhalte auf Audio-CD mit dem CD-Brenner eines PCs kopierbar sind, kann man selbst von einer Kopie mit sich wechselndem Kopierschutzbit weitere Kopien anfertigen. Die auf der CD vorhandenen Daten werden beim Brennvorgang nicht ausgewertet, sondern einfach 1:1 kopiert, womit der Inhalt des Kopierschutzbits für den Kopiererfolg unbedeutend ist.

- Einige Audio-Recorder (insb. solche für den professionellen und semiprofessionellen Bereich) werten das SCMS-Kopierschutzbit auf Wunsch des Nutzers nicht aus bzw. setzen es nach Bedarf.

  Unter http://www.american-digital.com/prodsite/product.asp?p=112&c=15 findet man beispielsweise die Produktbeschreibung des Marantz CDR631. Dort steht „SELECTABLE COPY PROTECTION: Bypass SCMS copy protection when duplicating a disc. Or set your own copy protection at the level you decide.“

- Am Markt sind Konverter erhältlich, die in den Signalweg zwischen Player und Recorder geschaltet werden und das SCMS-Kopierschutzbit nach Wunsch setzen.

  Unter http://www.midiman.net/products/m-audio/co3a.php wird beispielsweise ein „Coaxial, Optical AES/EBU Converter“ beschrieben. Zu SCMS steht dort: „Control over SCMS. If you use Minidisc technology, you probably know that your discs are encoded with SCMS (Serial Copy Management System), a kind of copy protection that prevents the data from being digitally copied. The CO3 gives you control over SCMS, enabling you to adjust those bits in the data stream to fit your needs.“

2.4.2 Regionale Kodierung

DVD-Medien und die zugehörigen Abspielgeräte besitzen Funktionen zur Auswertung eines sog. „Ländercode“, der der künstliche Marktseparation dient. In die Player-Hardware ist ein Schutzmechanismus integriert, der das Entschlüsseln verschlüsselter DVDs nur dann ermöglicht, wenn das Abspielgerät einen passenden Ländercode besitzt. Die Hersteller von DVD-Spielern haben meist das Ändern dieser Ländercodes vorgesehen, aber das Wechseln des Ländercodes auf eine maximale Anzahl begrenzt.

Hiermit bezweckt man, dass Inhalte, die in einem anderen Land oder Erdteil früher als in anderen auf den Markt kommen, nicht vorzeitig in anderen Ländern verbreitet werden. Da das Preisgefüge von Land zu Land sehr unterschiedlich sein kann (DVDs sind in den USA im Mittel etwa 30 Prozent günstiger als in Europa), will man die durch Export und Niedrigpreise entstehenden „Verluste“ begrenzen.

Einige Abspielgeräte besitzen jedoch Funktionen, mit denen man die Firmware des DVD-Spielers patchen kann, so dass der Ländercode (zwar umständlich), aber beliebig oft geändert werden kann. Entsprechende Software kann im Internet kostenlos heruntergeladen werden. Teilweise werden auch Geräte verkauft, die den Ländercode überhaupt nicht auswerten. Entsprechende Gerätelisten findet man in Internet beispielsweise unter http://www.zonefreedvd.com/ und http://www.codefreedvdplayers.com/.

Insofern schützt der Ländercode nicht perfekt und schon gar nicht vor ernsthaften „Knackversuchen“, Gelegenheitstäter werden jedoch abgeschreckt. Im Übrigen führt der Preisverfall bei Player-Hardware dazu, dass man sich künftig mehrere Abspielgeräte (oder Laufwerke im PC) leisten können wird.

2.4.3 Nichtkompatible Medien

Die für jedermann leichte und ohne Qualitätsverlust mögliche Kopierbarkeit der Audio-CD ist in erster Linie darauf zurückzuführen, dass in der Form von CD-ROM-Laufwerken heute billigste Audio-CD-Abspielgeräte vorliegen, mit deren Hilfe PC-Software direkt auf die digitalen Rohdaten des Mediums zugreifen kann. Dieses Problem könnte auf den ersten Blick dadurch umgangen werden, dass die Industrie sich darauf einigt, grundsätzlich ausschließlich physikalisch völlig inkompatible Medien für das Abspielen urheberrechtlich geschützter geistiger Werke auf der einen Seite und als Speichermedien für Universalcomputer auf der anderen Seite zu verwenden. Die Einhaltung derartiger Absprachen könnte ggf. in Form von entsprechenden Lizenzbedingungen für die der Speichertechnologie zugrunde liegenden Patente mit existierenden rechtlichen Mitteln gesichert werden.

Dieser Ansatz widerspricht natürlich völlig dem Ziel und Anspruch der Multimedia-Idee, demzufolge für den Konsumenten erhebliche neue und attraktive Möglichkeiten gerade durch die Integration aller verfügbaren Medien mit den flexiblen Softwaremöglichkeiten eines Universalcomputers (PC) entstehen. Nichtkompatible Medien bieten natürlich auch keine Schutzlösung für PC-Software, da diese immer in einem für den Computer lesbaren Format ausgeliefert werden muss.

2.4.4 Ausnutzung historischer Inkompatibilitäten

Angesichts des großen Interesses der Musikverlage, den Austausch komprimierter Musik-CDs über das Internet zu erschweren, wurden von zahlreichen Unternehmen verschiedene Schutztechniken für das existierende CD-System ersonnen (siehe z.B. [33]). Alle diese Verfahren basieren auf historisch bedingten kleinen Unterschieden im Verhalten von CD-ROM-Laufwerken in Computern und Audio-CD-Spielern. CD-ROM-Laufwerke sind in der Regel mit moderner Software ausgestattet und unterstützen mehr Kodieralternativen als die oft wesentlich älteren und einfacheren integrierten Schaltungen in Audio-CD-Spielern. Audio-CDs, die unter Anwendung dieser Schutzsystemen hergestellt wurden, verletzen gezielt die Spezifikation des CD-Standards in einer Art und Weise, welche von einfachen Abspielgeräten ignoriert wird, aber in Computerlaufwerken zu Fehlfunktionen führt. Beispiele dafür sind bestimmte sehr gezielt eingebrachte Bitfehler im Audiodatenstrom oder verwirrende Eintragungen in den Inhaltsverzeichnisdaten oder Zeitmarkierungen der CD.

Diese Techniken sind mit einer Reihe von Risiken verbunden. Zum einen erwartet ein Kunde, der eine Audio-CD erwirbt, natürlich, dass es sich dabei um ein korrekt der CD-Spezifikation entsprechendes Produkt handelt, und nicht um ein „gepanschtes“ Medium. Das Abspielen einer Audio-CD auf einem CD-ROM-Laufwerk ist ja für sich eine durchaus legitime Nutzung des Produktes, weshalb diese Art von Kopierschutz durch künstlich provozierte Inkompatibilität als Produktmangel gewertet werden und mit den entsprechenden Verbraucherschutzrechten angegangen werden kann. Auch lässt sich eine Unterscheidung zwischen CD-ROM-Laufwerken und Audio-CD-Abspielgeräten nicht immer klar und ohne Ausnahmen durchführen, da heute beide Arten von Geräten nicht selten auf den gleichen Schaltkreisen beruhen, weshalb der Kopierschutz auch die Käufer einiger neuerer reiner Audio-CD-Abspielgeräte treffen könnte. Aus diesem Grund werden gezielte Verletzungen des CD-Standards von Musikverlagen bislang nur in kleinen Pilotversuchen getestet.

Hinzu kommt noch, dass mit speziellen Programmen, die auf das „Clonen“ (Vervielfältigen eines Datenträgers inkl. etwaiger Fehlerstellen) spezialisiert sind, meist doch Kopien angefertigt werden können. Weitere Informationen zu Kopiervorrichtungen finden sich in Abschnitt 3.6.1.

2.4.5 Aufspüren von illegalen Inhalten

Soweit möglich, sollten die Schutzmechanismen Urheberrechtsverletzungen von vornherein verhindern. Da dies nicht perfekt möglich ist, wird es in der Praxis doch zu Piraterie und illegalem Angebot fremder Inhalte kommen. Im Folgenden werden Möglichkeiten zum Aufspüren und Verfolgen solcher Urheberrechtsverletzungen skizziert, bewertet und ihre Grenzen aufgezeigt. Die geschilderten Techniken (sowohl zum Aufspüren als auch zum Schutz davor) kommen ebenfalls bei anderen Tatbeständen (z.B. Aufspüren und Verfolgen von Kinderpornographie) zum Einsatz.

Die Tatsache, dass digitale Inhalte verlustfrei kopierbar sind, kann man sich zunutze machen: Jeder unveränderte Inhalt besitzt exakt das gleiche Bitmuster wie sein Original. Deshalb genügt eine einfache Vergleichsoperation über alle Inhalte auf Webservern, Datenbanken, File-Sharing-Systemen etc., um illegal abrufbare fremde Inhalte aufzuspüren. Hierzu verwendet man einen Scanner, der die erreichbaren Inhalte analysiert. Im Internet (hier: World Wide Web) könnte ein solcher Scanner z.B. in Kombination mit einer Suchmaschine (Web-Robot) betrieben werden, die ohnehin jeden erreichbaren Inhalt abruft und analysiert, in diesem Fall proaktiv, d.h. ohne konkreten Verdacht, dass tatsächlich eine Rechtsverletzung vorliegt.

In der Praxis gelten natürlich ein paar Einschränkungen bzgl. des erreichbaren Schutzes durch Scannen:

- Sollen die illegalen Inhalte nicht öffentlich, sondern illegal in einer geschlossenen Benutzergruppe angeboten werden, kann sie der Pirat verschlüsseln und sie somit vollständig vor dem Aufspüren schützen.
- Es ist möglich, das wahre Datenformat eines Inhalts unkenntlich zu machen (z.B. durch so simple Methoden wie Umbenennen einer Dateiendung von .mp3 zu .txt oder durch Entfernen von Headerinformation innerhalb der Datei), sodass der Scanner sie als nicht relevant einstuft. Hintergrund ist die Tatsache, dass der Scanner wegen des riesigen Datenvolumens zur Optimierung der Suchleistung nur nach typischen Dateitypen, z.B. Vi-

deos (.avi, .mov), Musik (.wav, .mp3), Bilder (.jpg) suchen wird. Hier hilft nur, alle Dateitypen nach den aufzuspürenden Bitmustern zu durchsuchen.

- Medienformate können (teilweise verlustfrei, teilweise verlustbehaftet) ineinander überführt werden, z.B. das Bildformat JPEG (.jpg) in das Format Portable Network Graphics (.png). Bei der vorhandenen Fülle an Medienformaten und Kodierverfahren müsste dann nach jedem möglichen Zielformat gesucht werden, was zu einer kombinatorischen Explosion der Möglichkeiten führt.

- Inhalte können neu digitalisiert werden, was aufgrund des stets vorhandenen Quantisierungsrauschens zu stochastischen Unterschieden zwischen Original und Kopie führen wird und nur durch inhaltsbasierte Analysen (also nicht den bloßen Vergleich von Bitketten, sondern durch „fortgeschrittene“ Methoden) und Extrahieren von Watermarks erkannt werden kann.

Hat man illegale Inhalte gefunden, können zusätzlich zu den möglicherweise bereits vorhandenen Beweisen noch die Protokolle (Log-Files) der Server, auf denen die Inhalte gefunden wurden, sichergestellt werden. Das Aufspüren von Rechtsverletzungen mittels Durchsuchen der vorhandenen Datenbestände muss natürlich auf legale Weise erfolgen, d.h. das Eindringen in fremde Server, um festzustellen, ob dort illegale Inhalte vorhanden sind, ist nicht erlaubt.

In diesem Sinn zwar wirkungsvoll, aber kritisch zu bewerten sind Methoden, bei denen man vorgeht wie ein Pirat: Eine Verfolgung ist theoretisch dadurch möglich, dass die Adressierungsinformation auf der Netzwerkebene verwendet wird, um den Anbieter bzw. Konsumenten zu verfolgen. Dies machen sich z.B. der Media Enforcer (http://mediaenforcer.tripod.com/enforcer/) und Zeropaid (http://www.zeropaid.com/busted) zunutze, um die IP-Adressen von Tauschhändlern herauszubekommen, z.B. indem sie Dateien mit eindeutig lautenden Dateinamen zum Download anbieten.

Unter http://dailynews.yahoo.com/h/zd/20011016/tc/riaa_we_ll_smother_song_swappers_1.html war im Internet weiterhin zu lesen, die Musikindustrie experimentiere mit einer neuen Methode gegen die Bereitstellung illegaler Inhalte im Internet, indem sie nach dem Aufspüren eines entsprechenden File-Sharing-Servers den Server blockieren könne und anschließend die Verbindungen zu Clients übernehme und die gewünschte Datei während des Downloads ausgetauscht werde. Ein Vorstoß seitens der RIAA (Recording Industry Association of America), solche Methoden im Rahmen eines im Oktober 2001 vom US-Kongress verabschiedeten Anti-Terror-Gesetzes zu legalisieren, scheiterten allerdings, berichtete das Online-Magazin Telepolis (http://www.heise.de/tp/deutsch/inhalt/te/9831/1.html).

Inhalte können auch durch bewusstes mehrfaches und langanhaltendes Abrufen den Server derart überlasten, dass er unter der Last zusammenbricht. Somit bekämen andere Interessenten keinen Zugriff zu den illegalen Inhalten mehr. Das Blockieren von Inhalten mit solchen Methoden ist gleichzusetzen mit einem Denial-of-Service Angriff und beeinträchtig somit alle Internet-Nutzer (auch solche, die den illegalen Inhalt nicht abrufen), da die Internet-Verbindungen verstopft werden. Gemäß der Task-Force „Sicheres Internet“ [29, 21] der Bundesregierung wäre ein solches Vorgehen seitens des Verfolgers höchstwahrscheinlich strafbar. Legalisierung würde in jedem Fall den Missbrauch von Denial-of-Service Angriffen fördern.

2.4.6 Zugriffsfilter und Sperren

Häufig stellen Internet Service Provider ihren Kunden speziell zugeschnittene Standarddienste zur Verfügung, bei denen eine grobe Vorauswahl der Inhalte und auch eine Sperrung bereits bekannter kritischer Inhalte erfolgt. Dies kann z.B. sinnvoll sein, wenn Eltern ihren Kindern den Zugang zum Internet ermöglichen wollen. So kann der Provider z.B. einen Filter für Spam-E-Mails, Werbe-E-Mails oder spezielle Webadressen (URLs) vorsehen, um seine Kunden nach ihren Wünschen zu schützen.

Umgekehrt betrachtet eigenen sich solche Filtermechanismen auch, um dem Nutzer den Zugang zu bestimmten Inhalten (z.B. rechts- oder sittenwidrige) zu verwehren.

Der Nutzer kann sich jedoch leicht über die Filterung hinwegsetzen, wenn er kein Filtern wünscht, was die Wirkung solcher gefilterter Dienstangebote teilweise in Frage stellt. Der Nutzer muss hierzu z.B. auf ungefilterte News-Server ausweichen, oder er benutzt sog. Proxy-Dienste (siehe auch Abschnitt 3.5).

Die Filterung von Inhalten setzt eine vorgeschaltete Bewertung nach vorgegebenen Kriterien (z.B. Qualität, Zulässigkeit, Rechtsverträglichkeit) voraus. Diese kann manuell (durch Menschen) oder automatisch (durch Maschinen) erfolgen.

Die automatisierte Kontrolle von Inhalten erfordert eine semantische Analyse von Daten. Computer sind jedoch bestenfalls in der Lage, syntaktische Auswertungen vorzunehmen. Folglich ist eine vollautomatische Filterung von Inhalten unmöglich. Halbautomatische Verfahren, d.h. eine Kombination von automatischer und manueller Bewertung sind jedoch möglich. Das Filtern von Inhalten ist selbstverständlich nur bei unverschlüsselter Nachrichtenübermittlung möglich.

Eine weitaus ausführlichere Diskussion zu den Folgen und der Wirkung von Sperrungen im Internet ist z.B. in [36] zu finden.

Automatische Bewertung aufgrund formaler Kriterien

Die einfachste und einleuchtendste Art der Bewertung ist das Überprüfen der Inhalte nach vorgegebenen Schlüsselworten. Dies eignet sich natürlich nur für Texte. Für Bilder und andere Medien bietet sich eine Überprüfung mit Hilfe von Checksummen an. Allerdings werden hier nur Inhalte erkannt, die dem Bewerter bereits vollständig bekannt sind und vom Sender nicht, d.h. nicht einmal in einem Bit, verändert wurden.

Ein Ansatz zu einer intelligenteren Bewertung von Inhalten ist das Content-based Database Retrieving (siehe z.B. http://wwwqbic.almaden.ibm.com), bei dem über die Angabe bestimmter Bildkriterien (z.B. Vorhandensein bestimmter Texturen, Farbzusammensetzung etc.) eine Bewertung möglich ist.

Im Audio-Bereich ist man inzwischen in der Lage, Musikstücke aus wenigen Sekunden Material zu erkennen.

Trotz der Fortschritte, die im Bereich der automatisierten Bewertung noch zu erwarten sind, können Fehleinschätzungen bei der automatisierten Bewertung in beide Richtungen auftreten: Einerseits können zu filternde Inhalte als einwandfrei erkannt werden, andererseits könnten auch Inhalte ohne Relevanz geblockt werden. Beispiele hierfür sind Diskussionsforen, die sich mit den Auswirkungen rechtswidriger, krimineller oder pornographischer Handlungen und Inhalte beschäftigen, ohne die Inhalte selber zum Gegenstand des Austauschs zu machen.

Manuelle Bewertung durch Dritte

Zunächst besteht natürlich die Möglichkeit, dass der Content Provider selbst seine Inhalte mit einer Bewertung versieht. Dies ist in Bereichen, in denen die Selbstregulierung greift, durchaus sinnvoll und hat in Systemen wie PICS (Plattform for Internet Content Selection) seine Berechtigung. Die Kombination mit dem unabhängigen Rating der Angebote durch unabhängige Dritte kann so eine qualitative Steigerung des Internetangebots nach sich ziehen, wie dies bei PICS der Fall ist. Infolge der Bewertung entstehen Sperrlisten, die entweder beim Provider oder auf dem lokalen Rechner des Benutzers vorhanden sind. Bei der Anforderung gesperrter Inhalte werden diese gar nicht erst vom Server angefordert. Filterkriterien, aus denen die Listen aufgebaut werden, können Rechneradressen (IP-Adressen), Webadressen (URLs), Namen von Newsgruppen, aber auch Message-IDs (besonders bei E-Mail und News-Beiträgen) sein.

Aufgrund der riesigen Datenmenge, die das Internet heute aufweist, ist eine vollständige Bewertung aller Inhalte aussichtslos. Die hinzukommende Dynamik der Inhalte macht eine dauerhafte und nachhaltige Bewertung unmöglich.

Rights Protection System (RPS)

Im Bereich Schutz der Urheberrechte wurde ebenfalls ein Filtersystem vorgeschlagen, um die illegale Verbreitung urheberrechtlich geschützter Materialien zu verhindern. Beim Rights Protection System [24] sollten die Internet Service Provider entsprechende Hard- und Software bei sich installieren.

Mit RPS wollte die Musikindustrie Grenzkontrollen im Internet einführen. Zugriffe aus Deutschland auf urheberrechtsverletzende Inhalte im Ausland sollten bei den wenigen deutschen Internet Service Providern mit einer Auslandsanbindung über einen den Routern vorgeschalteten Filter unterbunden werden. Dies sind in Deutschland nur etwa 50–70 Stellen.

RPS hat sich jedoch nicht durchgesetzt, einerseits wegen der hohen Kosten, andererseits wegen der generellen Kritik an Sperren und ihrer Wirkungslosigkeit gegenüber ernsthaften Umgehungsversuchen (siehe auch Abschnitt 3.5). Große Kritik gab es auch an dem Vorschlag, das RPS auf einem innerdeutschen zentralen Knotenpunkt, dem de-cix, zu installieren, da eine dortige Installation von RPS nicht der Grenzkontrolle, sondern die Überwachung des innerdeutschen Internetverkehrs gedient hätte.

3 Angriffstechniken und -werkzeuge

Trotz aller Bemühungen zeigen sich bei den existierenden Schutzsystemen immer wieder Schwächen, die von intelligenten Angreifern ausgenutzt werden, um Urheberrechte zu verletzen. Diese Schwächen lassen sich einteilen nach

- systematische Schwächen der Systeme und
- Schwächen bzw. Angriffsmöglichkeiten, die durch ungeeignete oder gar fehlerhafte Mechanismen hervorgerufen werden.

Oft haben auch der enorme Konkurrenzdruck und die immer kürzer werdenden Time-To-Market-Zyklen damit zu tun, dass Schutzsysteme bereits gebrochen sind, bevor sie weite Verbreitung erlangt haben. Die folgenden Abschnitte beschreiben typische Vorgehensweisen und Schwächen existierender Schutzsysteme.

3.1 Angriffe auf die verwendete Kryptographie

Kryptographische Mechanismen (siehe Abschnitt 2.2.1) sind, wenn sie gut gewählt und sorgfältig von Experten untersucht sind, aller Voraussicht nach nicht zu brechen. Die heute aktuellen Verfahren können daher guten Gewissens auch in DRM-Systemen zum Einsatz kommen.

3.1.1 Brechen der kryptographischen Mechanismen

Man unterscheidet verschiedene Stufen des Brechens kryptographischer Verfahren:

- **Vollständiges Brechen:** Finden des Schlüssels,
- **Universelles Brechen:** Finden eines zum Schlüssel äquivalenten Verfahrens,
- **Nachrichtenbezogenes Brechen:** Brechen für einzelne Nachrichten, ohne den Schlüssel selbst in Erfahrung zu bringen.
  - Selektives Brechen: für eine vom Angreifer bestimmte Nachricht (z.B. einen abgefangenen Schlüsseltext),
  - Existenzielles Brechen: für irgendeine Nachricht.

Dabei ist zu unterscheiden, ob ein Angreifer lediglich eimalige Kosten hat, um den verwendeten Schlüssel effizient knacken zu können, oder jeder Angriff auf eine Nachricht signifikante Kosten beim Angreifer verursacht. Ein Angreifer wird im Normalfall versuchen, an der schwächsten Stelle des Systems anzugreifen. Meist sind Angriffe auf die verwendete Kryptographie weniger aussichtsreich als z.B. das direkte Abgreifen des Klartextes (ggf. auch in leicht verminderter Qualität) oder Angriffe auf die physischen Sicherungsmaßnahmen (siehe Abschnitt 3.2) zur Geheimhaltung des Entschlüsselungsschlüssels.

3.1.2 Sicherheit aktueller Verfahren

Seit einigen Jahren existieren einige Kryptoalgorithmen, die nach dem Stand der Wissenschaft als *praktisch sicher* bezeichnet werden können. Praktisch sicher bedeutet, dass für den jeweiligen Algorithmus nach dem aktuellen Kenntnisstand keine effizienten Kryptanalyseverfahren bekannt sind. Zu diesen Algorithmen zählen z.B.:

- Triple-DES (Triple Data Encryption Standard) mit einer Schlüssellänge von 112 Bit,
- Rijndael, der neuer amerkanischer Verschlüsselungsstandard AES (Advanced Encryption Standard) ist, mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit,
- IDEA (International Data Encryption Algorithm) mit einer Schlüssellänge von 128 Bit,
- RSA, ein asymmetrischer Algorithmus, mit einer Schlüssellänge (Moduluslänge) von mindestens 1024 Bit.

Der in die Jahre gekommene DES (Data Encryption Standard) ist mit seiner geringen Schlüssellänge von 56 Bit nicht mehr sicher.

In jedem Fall können diese Algorithmen immer noch durch sog. **vollständiges Durchsuchen des Schlüsselraumes** (auch *Brute-force Attack* genannt) gebrochen werden. Wie aufwendig das praktisch ist, hängt von der Schlüssellänge des jeweiligen Algorithmus ab. Dabei ist zu beachten, dass die Schlüssellänge nie losgelöst vom Algorithmus betrachtet werden kann. So erreicht der asymmetrische Algorithmus RSA mit einer Schlüssellänge von 1024 Bit momentan etwa das gleiche Sicherheitsniveau wie der symmetrische IDEA mit 128 Bit.

Bei symmetrischen Systemen gelten derzeit 128 Bit Schlüssellänge als ausreichend. Wie hoch der finanzielle und zeitliche Aufwand für das Brechen eines symmetrischen Systems in Abhängigkeit der Schlüssellänge im Jahr 1995 war, zeigt die Tabelle 3.1 (nach [52, S.153]).

	Schlüssellänge in Bit					
Kosten in USD	40	56	64	80	112	128
100.000	2 s	35 h	1 Jahr	70.000 Jahre	10^{14} Jahre	10^{19} Jahre
1.000.000	0,2 s	3,5 h	37 d	7.000 Jahre	10^{13} Jahre	10^{18} Jahre
10.000.000	0,02 s	21 min	4 d	700 Jahre	10^{12} Jahre	10^{17} Jahre
100.000.000	2 ms	2 min	9 h	70 Jahre	10^{11} Jahre	10^{16} Jahre

Tabelle 3.1: Zeitlicher Aufwand für eine hardwarebasierte Brute-force Attack

Weiterhin hängt die notwendige Schlüssellänge von der Zeitdauer ab, die eine Information unbedingt geschützt bleiben muss. Muss die Information nur wenige Minuten bis Stunden

geschützt bleiben, z.B. weil sie anschließend sowieso öffentlich wird, genügen Schlüssellängen zwischen 64 und 128 Bit. Dies sind z.B. gebräuchliche Werte für Sitzungsschlüssel im Broadcasting. Für längerfristige Geheimhaltung sind heute Schlüssellängen ab 128 Bit zu wählen.

Nachdem kryptographische Algorithmen oder ganze Systeme veröffentlicht wurden, werden teilweise Fehler im Design entdeckt, die zur Unsicherheit führen. Grundsätzlich ist von der Nutzung selbst designter Krypto-Algrithmen abzuraten, wenn sie nicht ausgiebig durch die Krypto-Community untersucht worden sind. Zu hoch ist die Wahrscheinlichkeit, dass dem Designer Fehler unterlaufen sind, die dann von Hackern gnadenlos ausgenutzt werden können.

Auch bei der Umsetzung (Implementierung) von Krypto-Algorithmen treten immer wieder Fehler auf. Meist sind dies Unachtsamkeiten (kleine Programmierfehler mit großer Wirkung) und Unwissen des Entwicklers bzgl. der exakten Funktionsweise des Algorithmus. Seltener werden neue Angriffe entdeckt: So können beispielsweise Verzweigungen des Programmcodes innerhalb des Ver- oder Entschlüsselungsalgorithmus zu einem Informationsgewinn beim Angreifer über den Schlüssel führen (timing analysis, [34]). Bei Smart Cards konnte durch Messung des Stromverbrauchs der Karte während eines Verschlüsselungsvorgangs ebenfalls der nur auf der Karte vorhandene Schlüssel ermittelt werden, obwohl dies die Smart Card eigentlich hätte verhindern sollen (power analysis, [35]). Darüber hinaus müssen Entwickler auch bedenken, dass Angreifer gerade bei Chipkarten versuchen können, durch gezielte Misshandlung des Prozessors Fehlfunktionen auszulösen, durch die Zugriff auf sicherheitskritische Informationen erlangt werden kann (fault induction, [2, 43]).

3.2 Schwächen manipulationssicherer Hardware

Wir müssen davon ausgehen, dass der Angreifer technisch gut ausgebildet ist und über Ausrüstung zur Untersuchung und Änderung von elektronischen Schaltungen und hochintegrierten Halbleiterbausteinen verfügt. Bevor jedoch konkrete Angriffe diskutiert werden, sollen zunächst Angreiferklassen (Gefährlichkeitsklassen) und Schutzklassen eingeführt werden.

3.2.1 Gefährlichkeitsklassen

In [1] werden die beim Entwurf eines Systems zu berücksichtigenden Angreifer entsprechend ihren Möglichkeiten in drei grobe Gefährlichkeitsklassen eingeteilt:

- **Klasse I: Clevere Außenstehende.** Sie sind oft sehr intelligent, haben aber nur beschränktes Wissen über den Aufbau des untersuchten Systems. Sie haben nur Zugang zu mittelmäßig aufwendiger Ausrüstung (z.B. Lötkolben, Mikroskop, einfache Chemikalien, mechanische Werkzeuge, PC, In-Circuit-Emulator und Logik-Analysator). Sie nutzen oft existierende Schwächen des Systems aus, anstatt neue zu schaffen. Beispiele sind Studenten, Hobbyelektroniker oder Privatdetektive.
- **Klasse II: Erfahrene Insider.** Sie haben eine gezielte technische Ausbildung und viel Erfahrung. Sie haben unterschiedlich gutes Wissen über die Bestandteile des untersuchten Systems, aber prinzipiell Zugang zu Beschreibungen der technischen Einzelheiten. Oft haben sie auch Zugang zu anspruchsvoller Ausrüstung zur Untersuchung des Systems. Beispiele sind einzelne Mitarbeiter eines Systemherstellers oder -betreibers.

- **Klasse III: Zahlungskräftige Organisationen.** Sie sind in der Lage, Spezialistenteams mit Experten verwandter und sich ergänzender Ausbildung zusammenzustellen, die mit großen finanziellen Mitteln ausgestattet sind. Sie können eine detaillierte Analyse des untersuchten Systems durchführen, anspruchsvolle Angriffe entwickeln und haben Zugang zu den aufwendigsten Untersuchungshilfsmitteln (Chiptestarbeitsplätze, Elektronenmikroskope, Plasmaätzanlagen, Röntgengeräte, Elektronenstrahltester, Ionenstrahlarbeitsplatz, UV Lasersystem, usw.). Sie können eventuell auf erfahrene Insider als Teammitglieder zurückgreifen. Beispiele für Klasse-III-Angreifer sind die Labors von Geheimdiensten, von großen Mikroelektronikherstellern und einige kriminelle Vereinigungen.

3.2.2 Klassifikation von Schutzmechanismen

Der Aufwand der Schutzmechanismen, die in einem manipulationssicheren System eingesetzt werden müssen, hängt von den geschätzten Fähigkeiten und Mitteln des Angreifers ab. In [1] wird die Klassifikation von Schutzmechanismen in die folgenden sechs Stufen vorgeschlagen, abhängig von den Kosten, die aufgewendet werden müssen, um den Sicherheitsmechanismus zu überlisten:

- **Null:** Keine speziellen Sicherheitsvorkehrungen. Beispiel: ein normaler Bürocomputer.
- **Niedrig:** Es existieren einige einfache Sicherheitsmechanismen, die sich jedoch mit üblichen Laborhilfsmitteln und Werkzeugen wie Kneifzange, Lötkolben, Mikroskop, usw. umgehen lassen.
- **Mittel-Niedrig:** Teurere Werkzeuge sowie gewisses spezielles Wissen werden für einen erfolgreichen Angriff benötigt. Die Werkzeugkosten können im Bereich von etwa 500 bis 5000 US-Dollar liegen.
- **Mittel:** Spezielle Ausrüstung sowie spezielles Können und Wissen werden für einen erfolgreichen Angriff benötigt. Werkzeuge und Ausrüstung können im Bereich 50.000 bis 200.000 US-Dollar kosten. Der Angriff kann zeitaufwendig, aber letztendlich doch erfolgreich sein.
- **Mittel-Hoch:** Die erforderliche Ausrüstung ist zwar verfügbar, aber sehr teuer in der Anschaffung und im Betrieb und kann ebenfalls zwischen 50.000 bis 200.000 oder mehr US-Dollar kosten. Spezielles Können und Wissen ist notwendig, um die Ausrüstung einsetzen zu können. Mehr als ein aufwendiger Vorgang kann zur Überwindung der Sicherheitsmechanismen notwendig sein, so dass mehrere Experten mit sich ergänzendem Wissen zusammenarbeiten müssen. Der Angriff könnte letztendlich erfolglos bleiben.
- **Hoch:** Alle bekannten Angriffsversuche waren erfolglos. Eine Untersuchung durch ein Team von Spezialisten ist erforderlich. Sehr spezielle Ausrüstung ist erforderlich, die zum Teil erst entworfen und hergestellt werden muss. Die Gesamtkosten des Angriffs können mehrere Millionen US-Dollar übersteigen und es ist unsicher, ob der Angriff erfolgreich sein wird.

Diese Klassifikation von Sicherheitsmechanismen ist sicher sehr wertvoll für den Anwender eines Sicherheitsmoduls, da eine handfeste Aussage über den für einen Angriff notwendigen

Aufwand getroffen wird. Organisationen, welche Sicherheitsprodukte zertifizieren, vermeiden jedoch gerne konkrete Aussagen über die minimal erforderlichen Kosten eines erfolgreichen Angriffs, da eine gute Idee, eine sehr versteckte Sicherheitslücke oder eine neu verfügbare Technologie ganz unerwartet die Kosten des günstigsten möglichen Angriffs erheblich reduzieren kann.

Für Zertifizierungszwecke wurde daher in einer entsprechenden US-Norm [23] eine alternative Grobklassifikation von Sicherheitsmaßnahmen für manipulationssichere kryptographische Module vorgenommen. In den vier FIPS-Sicherheitslevels werden nur grundlegende Anforderungen an die Aufgaben der implementierten Schutzmechanismen gestellt, jedoch keine Aussagen über die Kosten eines Angriffs gemacht:

- **Sicherheitslevel 1:** Es werden nur Anforderungen an die verwendeten kryptographischen Algorithmen gestellt. Es werden keine besonderen physikalischen Schutzmaßnahmen verlangt, die über die normalen bei elektronischen Geräten üblichen geschlossenen Gehäuseformen hinausgehen.

- **Sicherheitslevel 2:** Das Sicherheitsmodul muss mit einem Siegel oder einem Schloss gesichert sein, oder in ein undurchsichtiges Material vergossen sein, so dass ein einfacher Manipulationsversuch durch die dabei entstandene Beschädigungen im Nachhinein offensichtlich wird.

- **Sicherheitslevel 3:** Ein Manipulationsversuch soll nicht nur im Nachhinein als Beschädigung erkennbar sein, sondern bereits während des Eingriffs vom Modul erkannt werden und zur sofortigen Vernichtung der im Sicherheitsmodul gespeicherten Geheimnisse führen. Ein einfaches Beispiel wäre ein sehr stabiles Gehäuse mit Schaltern, die beim Abnehmen des Gehäusedeckels sofort die gespeicherten Schlüsseldaten löschen, oder das Vergießen der Schaltung in sehr hartem Epoxid-Harz, um eine Beschädigung der Schaltung bei der Untersuchung wahrscheinlicher zu machen.

- **Sicherheitslevel 4:** Mit gewissem mechanischem Aufwand kann es immer noch relativ leicht möglich sein, die Alarmmechanismen von Level-3-Modulen zu umgehen, beispielsweise indem dünne Löcher an den Sensoren vorbei durch das Gehäuse gebohrt werden, über die der Zugang erfolgt. Level 4 verlangt einen umfassenden Eindringschutz von allen Seiten her. Das Eindringsensorsystem muss das Modul wie eine lückenlose Schutzhülle umgeben und im Falle eines Angriffs die Geheimdaten sofort löschen. Darüber hinaus muss durch Tests sichergestellt werden, dass bei variablen Umwelteinflüssen wie etwa Temperatur- und Spannungsschwankungen keine die Sicherheit des Moduls gefährdenden Systemzustände eintreten können. Alternativ können Sensoren eingesetzt werden, die bei ungewöhnlichen Umweltbedingungen wie etwa extremer Kälte eine Löschung der Geheimdaten auslösen.

Im Folgenden sollen nun konkrete Schwächen von manipulationssicherer Hardware und Ansatzpunkte für Angreifer beschrieben werden.

3.2.3 Einchip-Systeme

Die Sicherheit von Einchip-Systemen (Abschnitt 2.2.3, Seite 27) wurde von den Herstellern ursprünglich nur dadurch begründet, dass dem Angreifer die Systembusleitungen nicht zugänglich sind und er daher nur über die externen Schnittstellen mit der Anwendungssoftware kommunizieren kann. Ferner wurde von den Herstellern darauf hingewiesen, dass in EEPROM-Speichern die geheime Software nicht optisch sichtbar ist und lediglich als sehr empfindliches Ladungsmuster aufbewahrt wird, das sich beim Abätzen der oberen Schutzschichten sofort verflüchtigen wird.

Dennoch haben seit etwa 1994 regelmäßig Pay-TV-Piraten aus Chipkartenprozessoren mit gewissem Aufwand die geheimen Daten ausgelesen. Das Epoxid-Harz, in das der Chip eingebettet ist, kann mit rauchender Salpetersäure ($> 98\ \%\ HNO_3$) aufgelöst und mit Aceton entfernt werden [5]. Salpetersäure kann chemisch die in Siliziumchips eingesetzten Materialien Silizium, Siliziumoxid, Siliziumnitrit und Gold nicht angreifen. Das für Leiterbahnen auf den Chip aufgedampfte Aluminium überzieht sich sofort mit einer resistenten Schutzschicht (Al_2O_3) und wird daher ebenfalls nicht geschädigt.

Schon normale EEPROM-Mikrocontroller, die nicht speziell für Chipkarten- oder Sicherheitsanwendungen ausgelegt sind, versuchen, das unbefugte Auslesen der Daten zu verhindern. Sie verfügen über eine spezielle EEPROM-Speicherzelle mit einem Sicherheitsbit. Falls es gesetzt ist, wird das einfache Auslesen über die Programmierverifikationsfunktion des Prozessors verhindert. Jedoch ist immer noch bei vielen Mikrocontrollern dieses Sicherheitsbit in einer EEPROM-Zelle außerhalb der Fläche des normalen EEPROM-Speichers untergebracht. Der Angreifer muss daher nur die Chipverpackung wie beschrieben entfernen, den EEPROM-Speicher mit Farbe abdecken und die restliche Chipfläche mit UV-Licht bestrahlen, um das Sicherheitsbit zu löschen, ohne die Programmdaten zu vernichten. Anschließend können die Daten über den Programmiermodus ausgelesen werden. Diese Technik ist auch für Klasse-I-Angreifer durchführbar. Chipkartenprozessoren für Sicherheitsanwendungen verfügen aber in der Regel über bessere Schutzmechanismen.

Auch wenn es sehr schwierig ist, die Potentiale der EEPROM-Speicherzellen einer zugänglichen Chipoberfläche direkt auszulesen, so ist es doch relativ leicht möglich, Zugriff zu den Busleitungen zu bekommen. Nachdem die Epoxid-Harz-Verpackung des Chips entfernt wurde, befindet sich zwischen der Metallisierungsschicht, in der die Aluminiumverbindungen zwischen den Transistoren liegen, und der Chipoberfläche nur noch eine Passivierungsschicht. Diese robuste isolierende Schutzschicht aus Siliziumnitrit oder Siliziumoxid schützt die tieferen Schichten vor Beschädigung, Umwelteinflüssen und Ionenmigration. Sie lässt sich aber sehr einfach durch UV-Laserbeschuss entfernen, wozu ein spezielles Mikroskop mit Laseraufsatz eingesetzt wird. Anschließend kann der Angreifer feine Mikroprobing-Metallnadeln unter einem stark vergrößernden Mikroskop auf einem vibrationsgedämpften Arbeitstisch auf die ihn interessierenden Busleitungen setzen. Diese 0,5–2 µm spitzen Nadeln können über einen Vorverstärker mit einem Logik-Analysator verbunden werden, der dann die Vorgänge auf dem untersuchten Prozessorbus aufzeichnet [37].

Ein aufwendigeres Untersuchungsverfahren sind Elektronenstrahltester, bei denen der Chip wie in einem Elektronenrastermikroskop abgetastet wird [22]. Die Anzahl und Energie der von den Primärelektroden des Kathodenstrahls aus der Chipoberfläche herausgeschlagenen Sekundärelektroden geben Auskunft über das lokale elektrische Potential. Auf dem Bildschirm

des Elektronenstrahltesters sind daher die Spannungen auf den Leitungen des Chips als Helligkeitsunterschiede erkennbar (Spannungskontrast). Ein ebenfalls aufwendigeres, aber inzwischen in zahlreichen Labors verfügbares sehr leistungsfähiges Verfahren sind Ionenstrahlanlagen (FIB) [14], mit denen von der Chipoberfläche mit etwa 10 nm Auflösung in einer Vakuumkammer Material abgetragen oder deponiert werden kann. Dadurch lassen sich nachträglich auf einer Chipoberfläche Schaltungsänderungen durchführen und größere und damit leichter zugängliche Kontaktflächen anbringen. Diese Verfahren können bei Integrationsdichten und Frequenzen eingesetzt werden, bei denen Mikroprobing-Nadeln unzureichend sind.

Durch Beobachten der Busleitungen des Prozessors kann der geheime Speicherinhalt mitprotokolliert werden. Alternativ kann auch der Prozessor angehalten werden, und über die Busleitungen wird aktiv vom Angreifer der Speicher ausgelesen. Anschließend wird der vorgefundene Maschinencode disassembliert und ausgewertet, womit der Angriff auf das Einchip-System erfolgreich war.

Eine inzwischen gängige Schutzmaßnahme sind einige zusätzliche Metallisierungsschichten. Diese können zwar prinzipiell mit Ionenstrahlmanipulationsanlagen umgangen werden, allerdings erhöhen sie den Arbeitsaufwand für den Angreifer doch erheblich, insbesondere wenn die Chipoberfläche vor Aufbringen der Metallschutzschichten poliert wurde, so dass darunter liegende Strukturen nicht mehr an ihrem Höhenprofil erkennbar sind. Gute Metallschutzschichten sind nicht einfach homogene Flächen, sondern ein dichtes Netz aus Sensorleitungen, welche von der darunter liegenden Elektronik auf Kurzschluss oder Unterbrechung überprüft werden.

Durch systematisches Abätzen dünner Schichten des Chips und anschließendem vollständigen Fotografieren der Oberfläche des Chips kann ein hochauflösendes dreidimensionales Modell des Chips erstellt werden, aus dem dann mit Bildverarbeitungstechniken die Netzliste der Schaltung rekonstruiert werden kann [6]. Derartige den Chip zerstörende Verfahren helfen dem Angreifer, in Hardware implementierte kryptographische Algorithmen zu verstehen und einen Ausleseangriff auf einen anderen noch intakten Chip mit identischem Layout vorzubereiten.

Angesichts dieser heute in vielen besseren Mikroelektroniklabors verfügbaren Techniken erscheint es ausgesprochen schwierig, Schutzmechanismen höchster Sicherheit auf Chipebene zu realisieren. Die meisten heutigen Chipkarten dürften daher nur die Sicherheitsstufe **Mittel** (siehe Seite 48 auf der Skala nach [1]) erreichen, einige wenige ausgefeilte Chips von sehr erfahrenen Herstellern erreichen **Mittel-Hoch**. Einige Mikroelektronik-Labors bieten sogar kommerziell das Auslesen von einigen **Mittel-Niedrig** und **Mittel** Einchip-Systemen in Chipkarten und anderen Systemen als Dienstleistung für etwa zehntausend US-Dollar pro Chip an.

Für Einchip-Systeme stellt daher [23] keine speziellen Anforderungen an Schutzmaßnahmen auf dem Chip selbst, sondern nur an die Verpackung des Chips. Im Sicherheitslevel 4 muss der Chip in ein hartes undurchsichtiges Material eingegossen werden, dessen Härte- und Adhäsionseigenschaften es sehr wahrscheinlich machen, dass bei einem Versuch, die Verpackung mechanisch zu entfernen, der Chip ernsthaft beschädigt wird. Die Löslichkeitseigenschaften des Vergussmaterials sind so mit den auf dem Chip verwendeten Substanzen abzustimmen, dass Versuche, das Verpackungsmaterial chemisch aufzulösen, auch den Chip angreifen werden.

Derartige Sicherheitsverpackungen sind inzwischen kommerziell erhältlich, so beispielsweise das *ChipSeal*-System der Firma Dow Corning [9], oder das *Si-Shell*-System der Firma Schlumberger. Das *ChipSeal*-System wurde ursprünglich für den Einsatz in US-Militärausrüstung entwickelt, findet aber inzwischen auch in Systemen der Unterhaltungselektronik Verwendung,

so etwa in dem inzwischen vom Markt verschwundenen DVD-Verleihsystem DIVX, das ein anderes und bislang nicht kompromittiertes Verschlüsselungssystem hatte als die DVD.

3.2.4 Sichere Verpackung ganzer Baugruppen

Bei derartigen Sicherheitsmodulen (siehe auch Abschnitt 2.2.3, Seite 28) ist zu beachten, dass SRAM-Bausteine ihren Speicherinhalt bei Raumtemperatur für einige Sekunden ohne Versorgungsspannung erhalten können [53, 28]. Die verbliebene Ladungsverteilung in den Feldeffekttransistoren reicht aus, um das Flip-Flop beim Wiedereinschalten in den alten stabilen Zustand zurückkehren zu lassen. Diese Ladungsverteilung wird durch thermisches Rauschen langsam verändert. Durch Kühlung der ganzen Baugruppe auf etwa $-50\,^{\circ}$ Celsius kann das thermische Rauschen soweit verringert werden, dass sich die Information manchmal stundenlang ohne Versorgungsspannung halten kann.

Ein Angreifer könnte das Modul abkühlen und ohne Rücksicht auf den Alarmmechanismus die Verpackung schnell entfernen. Dann würde er den Kurzschluss, den der Alarmmechanismus ausgelöst hat, beseitigen und eine externe Versorgungsspannung anlegen, um anschließend das Modul auszulesen. Als Gegenmaßnahme sollte daher ein Sensor bei einer Abkühlung deutlich unter übliche Temperaturen ein Überschreiben der Daten auslösen.

Mit dieser Technik lassen sich Sicherheitsmodule entwickeln, die den FIPS Level 4 Anforderungen genügen, und auch einem Klasse-III-Angreifer einiges Kopfzerbrechen bereiten dürften. Ein möglicher Angriff wäre, bei Raumtemperatur mit speziell entwickelten Werkzeugen in Sekundenbruchteilen die Alarmmechanismen und die Batterie mechanisch abzutrennen, um ein aktives Überschreiben der Daten zu verhindern und dann sofort die Speicherbausteine mit einer externen Betriebsspannung zu versorgen. Ein anderer Angriffsansatz wäre, mechanisch die Drähte teilweise freizulegen, um mit einem sehr empfindlichen Spannungsmessgerät die Drahtwindungen nahe der Alarmschaltung ausfindig zu machen. Die an diesen Windungen anliegenden Potentiale werden dann mit einer externen Präzisionsspannungsquelle festgehalten, woraufhin der Angreifer die zwischen den extern spannungsstabilisierten Windungen liegenden anderen Drahtwindungen unterbrechen und den freigewordenen Raum für einen Zugang zum Inneren des Moduls nutzen kann.

Das physikalische Sicherungssystem des *IBM 4758 Transaction Security System* Moduls, das beispielsweise in vielen Geldautomaten eingesetzt wird, ist kurz in [1] beschrieben. Die äußere Schutzhülle besteht aus einer flexiblen Polyuretan-Folie, in die mehrere Lagen eines mit dotiertem und damit elektrisch leitfähigen Polyuretan gedruckten Sensorleitungssystem eingebettet werden. Da sich Leiter und Isolator chemisch nur geringfügig unterscheiden, ist es nicht mehr praktikabel, mit chemischen Mitteln wie beim Vorläufersystem die Drähte freizulegen und kurzzuschließen. Diese Alarmfolie umgibt die sicherheitsrelevanten Speicher-, Prozessor- und Verschlüsselungsbausteine völlig und schließt die Baugruppe hermetisch dicht ab. Die Widerstandsüberwachungsschaltung entspricht der in [56] beschriebenen. Das IBM 4758 Sicherheitsmodul war das erste nach FIPS Level 4 zertifizierte Sicherheitsmodul und dürfte nach einhelliger Ansicht von Fachleuten auch einem Klasse-III-Angreifer erhebliche Schwierigkeiten bereiten.

Das Schutzmembransystem, das die Firma Gore in Zusammenarbeit mit IBM für das IBM 4758 Modul entwickelte, ist inzwischen unter der Markenbezeichnung *D^3 Electronic Security Enclosure* auf dem Markt erhältlich [27] und verschiedene Hersteller arbeiten am Einsatz dieser

Schutztechnologie in wesentlich kleineren und kostengünstigeren Modulen als der etwa 2000 USD teuren für Bankanwendungen entwickelten IBM 4758.

Ein kleineres und wesentlich billigeres manipulationssicheres System ist der *iButton* der Firma Dallas Semiconductor (inzwischen Maxim). Dieses Modul ist eine kleine Stahlbüchse (5 mm hoch, 16 mm Durchmesser, einer Knopfzell-Batterie ähnlich), in der sich neben einer langlebigen Li-Batterie ein Sicherheitsmikroprozessor mit Metallschutzabdeckungen befindet, der seine Daten in batteriegepuffertem statischen RAM hält, welcher von mehreren Alarmmechanismen beim Öffnen der Büchse oder Verletzen der Chipoberfläche gelöscht wird.

Zusammenfassung

Zusammenfassend lässt sich sagen, dass die Entwicklung von für den Einsatz in der Unterhaltungselektronik geeigneten manipulationsresistenten Mikroprozessoren und Modulen derzeit noch am Anfang steht, es aber in den letzten fünf Jahren in diesem Bereich schon vielversprechende Fortschritte und eine erste Produktgeneration gegeben hat. Manipulationssichere Einchipsysteme sind insbesondere durch ihren niedrigen Preis (nur unwesentlich über dem anderer hochintegrierter Schaltungen) und ihre einfache Einsetzbarkeit mit konventioneller Bauteilebestückungstechnologie attraktiv für Hersteller, allerdings fehlt ihnen in der Regel der umfassende und ständig aktive Alarmmechanismus, der zum Schutz gegen Klasse III Angreifer wünschenswert ist, wie er bei Einsatz langlebiger identischer Schlüssel in einer großen Zahl von Abspielgeräten erforderlich wäre.

Die vielversprechendsten Schutzmaßnahmen für Einchipsysteme ohne dauerhafte Energiequelle sind extrem harte und gut mit dem Chipmaterial verbundene Verpackungsmaterialien, sowie obskure nicht-standard Schaltungstechniken und aufwendige Hardware-Implementationen der eingesetzten geheimzuhaltenden Sicherheitsmechanismen, um ein erfolgreiches Reverse Engineering so gut wie möglich zu erschweren, indem nicht nur Software, sondern auch Hardwareelemente rekonstruiert werden müssen.

Vielversprechender gegen Klasse-3-Angreifer sind aktive Schutzsysteme, die ggf. ganze Baugruppen, in welchen Schlüsseldaten in batteriegepufferten flüchtigen Speichern gehalten werden, hermetisch geschlossen umgeben und die bei Penetration der Schutzmembran die geschützten Daten umgehend dauerhaft löschen. Derartige Systeme erfordern aber nicht nur eine langlebige Batterie, sondern auch spezialisierte Fertigungstechnologie. Die einhergehenden Zusatzkosten von derzeit wohl mindestens 5–30 EUR pro Abspielgerät, das Risiko von verlorenen Daten durch Fehlalarme, sowie die batteriebedingt limitierte Lebensdauer von etwa einem Jahrzehnt machen diese im Prinzip heute schon ansatzweise verfügbaren Schutztechnologien noch etwas problematisch im breiten Einsatz in der Unterhaltungselektronik.

3.3 Schwächen von Watermarking-Systemen

Die Sicherheit von Watermarking-Verfahren gegenüber ernsthaften Angreifern lässt noch erheblich zu wünschen übrig. Es ist davon auszugehen, dass alle heute bekannten und alle zu erwartenden Watermarking-Systeme gebrochen werden in dem Sinne, dass Tools im Internet bereitgestellt werden, die das Watermark entfernen, ohne das Werk dabei wesentlich mehr zu verfälschen, als dies ursprünglich durch das Einbringen des Watermark geschehen ist.

3.3.1 Angriffe durch Transformationen

Eine generische Angriffsform besteht darin, das markierte Material so zu transformieren, dass es für den menschlichen Betrachter nur unwesentlich an Wert verliert, zugleich aber ein einfacher Detektor nicht mehr in der Lage ist, das Wasserzeichen zu erkennen. Die meisten Watermarkingleseverfahren lassen sich nicht durch die einfache Addition von sublimalen Störsignalen und Rauschen verwirren und überstehen dadurch beispielsweise die Quantisierungseffekte von verlustbehafteten Bildkompressionsverfahren wie JPEG meist unbeschadet. Jedoch reagieren sie oft sehr empfindlich auf selbst geringe und kaum wahrnehmbare geometrische oder zeitliche Verzerrungen, da sich dadurch Synchronisationspunkte verschieben.

Arbeiten mit dem Watermarking-Testprogramm StirMark [39] haben beispielsweise aufgezeigt, dass selbst viele Watermarkingverfahren, die noch gegen eine einzige geometrische Verzerrung eines Bildes robust waren (leichte Verschiebung, Streckung, oder Rotation), nach einer Kombination mehrerer solcher nichtwahrnehmbarer Schritte oder dem Einsatz von Verzerrungen, die bei der Entwicklung nicht berücksichtigt wurden (Scherung, Blähung, etc.), das Watermark nur noch in seltenen Fällen finden konnten. Ein über ein Bild gelegtes Gitter (siehe Abbildung 3.1) macht dies deutlich.

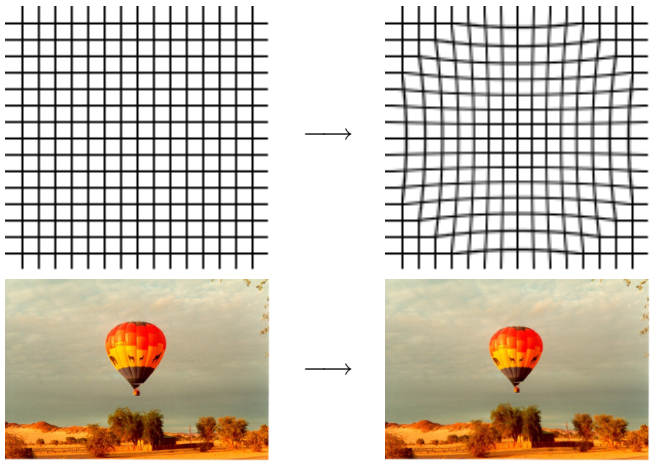

Abbildung 3.1: Stirmark Attack: Verbeulen eines Bildes

Das Watermark wurde dabei nicht wirklich entfernt und konnte nach Rücktransformation wieder zweifelsfrei nachgewiesen werden; es wurde nur für einfache und effiziente Detektoren unkenntlich. Spezielle forensische Watermarkingdetektoren sind durchaus in der Lage, eine große Zahl von Transformationsparametern auszutesten, um ein verbogenes Watermark wieder erkennbar zu machen, aber diese erfordern erhebliche Rechenzeit und lassen sich nicht praktikabel als billige Zusatzfunktion in einfachen Spielern einsetzen.

Solche Resultate zeigen, dass noch einiges an Forschungs- und Entwicklungsarbeit geleistet werden muss, bevor Watermarking-Verfahren ernsthaft gegen intelligente Angriffe sicher sind.

3.3.2 Mosaic-Angriff

Manchmal lassen sich gut gedachte Schutzmechanismen auch mit sehr primitiven, aber clever eingesetzten Mitteln aushebeln: Die Mosaic Attack [47] ist hierfür ein Beispiel. Watermarking-

Verfahren gehen davon aus, dass Manipulationen eines Inhaltes – z.B. Ausschneiden und Zerschneiden eines digitalisierten Fotos – das Watermark nicht unkenntlich machen sollen. Dies gelingt natürlich nur, wenn der Angreifer einen bestimmten Schwellenwert nicht überschreitet. Dieser sollte vom Urheber typischerweise so gewählt sein, dass der Bildinhalt für einen Piraten unbrauchbar bzw. nicht mehr wertvoll ist, wenn er den Schwellenwert überschreitet. Sobald der Angreifer einen sehr kleinen Bildausschnitt weiterverwendet, ist das Watermark nicht mehr detektierbar.

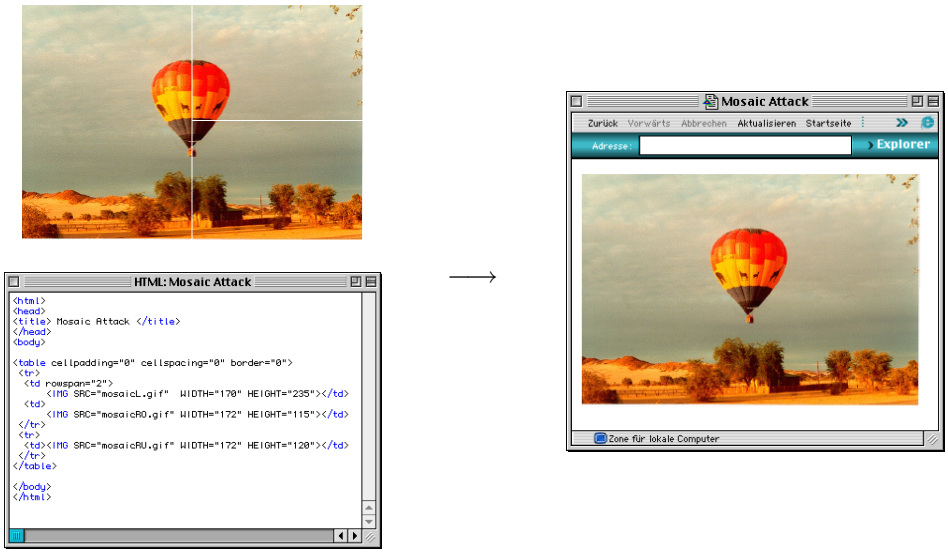

Abbildung 3.2: Mosaic Attack: Zerlegen eines Bildes

Die Mosaic Attack macht sich genau dies zunutze, allerdings so, dass der gesamte Bildinhalt ohne Verlust reproduzierbar ist, das Watermark aber trotzdem unerkennbar wird. Hierzu wird das Bild in viele kleine „Mosaikbausteine“ zerhackt, die anschließend für den Detektionsalgorithmus selbst dann unerkannt bleiben, wenn sie über einen geeigneten Mechanismus wieder zusammengesetzt und für den Betrachter zum ursprünglichen Bild reproduziert werden. Dies gelingt z.B. mit einer HTML-Seite, die aus einer (unsichtbaren) Tabelle besteht, deren Zellen die Mosaikbausteine (Teilbilder) enthalten (siehe Abbildung 3.2).

Ein Watermarkingleser darf daher beispielsweise bei HTTP-Zugriffen nicht auf einzelnen Bilddateien arbeiten, sondern muss die komplette Darstellungskette im Endgerät nachvollziehen (z.B. HTML-Layout, Java/JavaScript Interpretation, usw.), was den Rechenaufwand um Größenordnungen erhöht und den Einsatz von automatischen Echtzeit-Watermarkinglesern auf Breitbandkommunikationskanälen zur automatischen Filterung von geschütztem Material wesentlich problematischer macht.

3.3.3 Sensitivitäts-Angriff

Die heute bekannten Watermarking-Algorithmen basieren alle auf der Annahme, dass der Angreifer keine Kenntnis des zum Erkennen notwendigen Geheimschlüssels hat. Ein wirklich effektives und robustes asymmetrisches Watermarking-Verfahren, bei dem (analog zur asymmetrischen Kryptographie) die Kenntnis der im Watermarkdetektor eingesetzten Algorithmen

und Parameter nicht auch sofort zu einer recht offensichtlichen Methode zum Entfernen des Watermarks führt, ist nach unserem Kenntnisstand heute weder verfügbar noch in Aussicht. Man könnte deshalb annehmen, Watermarking-Verfahren müssten auch auf manipulationssichere Detektoren, die nicht für Reverse Engineering zugänglich sind, vertrauen.

Doch selbst bei Einsatz einer völlig geschützten Verpackung für den Detektor, kann dieser immer noch vom Angreifer zum Entfernen des Watermarks eingesetzt werden [13]. Dazu sucht der Angreifer mit einer Binärsuche zwischen einem Input mit und ohne Watermark nach einem Zwischenpunkt, an dem der Detektor gerade zwischen *Watermark vorhanden* und *nicht vorhanden* umschaltet. Anschließend wird die Eingabe so lange manipuliert, bis klar wird, welche lokalen Änderungen das Watermark erkennbar oder unkenntlich machen. Diese werden dann auf das markierte Bild angewendet, und somit wurde die kleinste Änderung angenähert, die das Watermark unkenntlich macht.

3.3.4 Weitere generische Angriffe

Viele erfolgreiche Angriffstechniken sind spezifisch für das jeweilige Watermarking-Verfahren, doch lassen sich auch einige weitere generische Verfahren nennen, welche die beschränkte Anwendbarkeit von Watermarking-Verfahren zu Kopierschutzzwecken verdeutlichen.

Sollte beispielsweise der Watermarking-Detektor nicht extrem sorgfältig in das Gesamtsystem integriert worden sein, so besteht die Gefahr, dass er einfach im Endgerät durch eine geringfügige Software- oder Hardware-Modifiktion deaktiviert wird, so dass sein – egal wie robustes – Ausgangssignal schlicht nicht mehr die illegitime Benutzung des Systems einschränkt.

Watermarks lassen sich durch Verschlüsselung der markierten Daten mühelos vollständig unkenntlich machen. Da moderne digitale Übertragungs- und Speichermedien mit beliebigen Bitströmen arbeiten, macht es für den Benutzer kaum einen Unterschied, ob Daten verschlüsselt oder im Klartext gehandhabt werden, insbesondere auf Universalcomputern und wenn die Verschlüsselung die Aktivierung unliebsamer inhaltabhängiger Kopierschutzmechanismen in Netzwerken und Speichergeräten ausschließt.

Watermarks für Videosignale bleiben oft über mehrere Einzelbilder hinweg konstant oder weisen andere Formen von Redundanz auf, um die notwendige Rechenleistung des Detektors zu beschränken. Da sich aber gleichzeitig die Bildinhalte rasch ändern, kann dies helfen, das Watermark vom Bild zu separieren. Ändert sich umgekehrt das Watermark von Einzelbild zu Einzelbild vollständig, so kann es durch Mittelung von sich weniger schnell ändernden Nachbarbildern abgeschwächt oder unkenntlich gemacht werden.

3.4 Reverse Engineering

Reverse Engineering von Systemen ist meist eine erlaubte Methode um zu verstehen, wie ein Mechanismus oder Gerät funktioniert und zudem eine sinnvolle Methode, um Schwächen zu finden, um die Systeme schrittweise zu verbessern. Der Verwertung der gewonnenen Erkenntnisse sind meist enge Grenzen gesetzt. Hierbei sollte man zusätzlich unterscheiden, ob durch Reverse Engineering speziell gesichertes Schlüsselmaterial oder lediglich ein Algorithmus, der vielleicht ohnehin patentrechtlich oder urheberrechtlich geschützt ist, an die Öffentlichkeit gerät. Bei derart geschützten Algorithmen ist auch der unberechtigte Nachbau illegal.

3.4.1 Nicht offengelegte kryptographische Algorithmen

Die Geheimhaltung von kryptographischen Verfahren – oftmals etwas geringschätzig als Security-by-obscurity bezeichnet – ist trotz gegenteiliger akademischer Lehrmeinung heute immer noch teilweise übliche Praxis, sowohl im kommerziellen als auch militärischen Bereich.

Eine der wesentlichen Grundanforderungen an moderne kryptographische Algorithmen ist, dass die gebotene Sicherheit ausschließlich auf der Geheimhaltung eines – im Notfall relativ leicht austauschbaren – kryptographischen Schlüssels beruhen soll. Alle weiteren Details des Verschlüsselungsverfahrens dürfen dem Gegner dagegen im Prinzip durchaus bekannt sein, ohne dass dadurch kryptoanalytische Angriffe praktikabel werden.

Dieses bereits 1883 von Kerckhoffs postulierte Prinzip [32] führte zur generellen Forderung nach einer vollständigen Offenlegung aller in sicherheitsrelevanten Anwendungen eingesetzten Kryptoalgorithmen. Dies ist auch heute zumindest im Bankwesen, bei digitalen Signatursystemen und bei Internet-Verschlüsselungssoftware dank entsprechender internationaler Standards weitgehend der Fall. Zahlreiche Fall-Beispiele belegen inzwischen auch deutlich, dass von kleinen und oft in der akademischen Kryptologie-Gemeinde nicht einschlägig bekannten „Experten“-Teams entwickelte und anschließend geheimgehaltene Verschlüsselungsverfahren oft erhebliche Schwächen aufweisen und nach Bekanntwerden von anderen Kryptologen oft innerhalb überraschend kurzer Zeit gebrochen werden, wie es beispielsweise beim Content Scrambling System (CSS) der DVD und verschiedenen Mobilfunk-Verschlüsselungsalgorithmen bereits geschehen ist.

Andererseits hat sich die Geheimhaltung der eingesetzen Algorithmen bei einigen Chipkarten-basierten Pay-TV-Systemen sogar als entscheidender Sicherheitsvorsprung bewährt. Bei Chipkartensystemen, in denen (in erster Näherung) alle Karten den gleichen Hauptschlüssel enthalten, ist der Schlüssel praktisch genauso gut oder schlecht austauschbar und vor Ausspähen geschützt wie der Verschlüsselungsalgorithmus. Der Einsatz eines bekannten Algorithmus gibt aber einem Angreifer mit verschiedenen Möglichkeiten zur Beobachtung und Manipulation der Hardware wichtige Informationen zur Planung und Durchführung eines Angriffs.

Einige Entwickler von Pay-TV-Chipkarten (z.B. NDS in Großbritannien) sind daher dazu übergegangen, in jeder Kartengeneration einen völlig neuen Verschlüsselungsalgorithmus als möglichst schwer durchschaubares Transistornetzwerk in Hardware zu implementieren. In der Praxis wird ein konkreter Angriffsversuch erheblich aufwendiger, wenn zunächst die Verdrahtung eines umfangreichen integrierten Schaltkreises rekonstruiert werden muss, um den zum Entschlüsseln notwendigen Algorithmus verstehen und auf den in einer Piratenkarte verwendeten Standardprozessor portieren zu können. Die eingesetzten Algorithmen werden dennoch nach Möglichkeit so gründlich geprüft werden müssen, dass sie selbst nach Bekanntwerden nicht notwendigerweise wesentlich unsicherer sind als bekannte Standardverfahren. Keinesfalls sollten durch die Geheimhaltung etwaige Schwächen des eigentlichen Algorithmus kaschiert werden, da dann Security-by-obscurity gegen ernsthafte Angreifer nichts helfen wird.

3.4.2 Reverse Engineering von Software

Reverse Engineering von DRM-Systemen ist nicht generell gleichzusetzen mit Piraterie. Beispielsweise könnte ein legal gekauftes und mittels eines DRM-Systems geschütztes Werk, das nur auf einem ganz bestimmten Betriebssystem oder einer Abspielsoftware nutzbar ist, den

verständlichen Wunsch seines Besitzers hervorrufen, es auch auf anderen Plattformen nutzbar zu machen.

Problematisch und keinesfalls von Dauer ist die durch „verworrenes Design“ erreichte Sicherheit von Softwarelösungen. Hierbei geht es lediglich darum, das Reverse Engineering des Programmcodes einigermaßen schwer zu machen.

Beispielsweise enthält der Microsoft Windows Media Player ein DRM-System (DRM2). Erwirbt der Nutzer eine Lizenz zum Abspielen eines Inhalts, kann er ihn jedoch nicht auf beliebiger Player-Soft- und -Hardware abspielen. Das DRM2-System wurde von Microsoft mit Blick auf erschwertes Reverse Engineering entwickelt. Eine (für den Außenstehenden) verworrene und unübersichtliche Struktur von Softwareobjekten soll die „Logik“ hinter dem System bestmöglich verstecken. Trotzdem ist es einem Programmierer gelungen, das System zu verstehen und ein Programm namens FreeMe [26] zu schreiben, mit dem Inhalte des Formats Windows Media Audio (WMA), für die eine Lizenz vorhanden ist, in einem auch für andere Player nutzbaren Format auf die Festplatte des Rechners abgespeichert werden können. FreeMe benutzt zum entschlüsseln die selben Funktionsaufrufe, die auch der Media Player nutzt, d.h. die DRM-Funktionen wurden nicht etwa „geknackt“, sondern vielmehr genutzt, um den Medienstrom abzuspeichern anstatt ihn auszugeben. Die technischen Details sind im Internet unter http://cryptome.org/ms-drm.htm veröffentlicht.

Ein weiteres Beispiel für den schwachen Schutz, den reine Softwarelösungen bieten, sind die in gängiger Abspielsoftware fehlenden Funktionen zum Abspeichern eines Medienstroms. Die Tatsache, dass eine Abspielsoftware (z.B. Windows Media Player oder Real Player) das Abspeichern nicht im Funktionsumfang anbietet, bedeutet keinesfalls, dass ein Pirat nicht in der Lage wäre, ein Programm zu schreiben, mit dem das Abspeichern möglich ist.

3.4.3 Begrenztheit reiner Softwarelösungen für DRM

Angesichts der weiten Verbreitung von Universalrechnern (PCs) und deren Multimedia-Möglichkeiten möchten die Inhalteanbieter verständlichweise auch diese Plattform mit Inhalten bedienen. Da PCs (zumindest bisher) sehr selten über entsprechende Hardware-Module verfügen, die zum Management der Rechte digitaler Daten geeignet wären, werden meist Lösungen für DRM in Software realisiert. In die Abspielsoftware oder sogar in die Betriebssystem-Software sind dann entsprechende DRM-Komponenten integriert. Nun leiden Softwarelösungen stets an dem Problem, dass die zu schützenden Geheimnisse, an denen die Sicherheit der DRM-Komponenten hängt, mehr oder weniger schutzlos dem Angreifer offenbart werden, da eine *physische* Kaselung in Software eben nicht möglich ist.

Insofern bleibt den Anbietern von Softwarelösungen nur ein Ausweg: Je verworrener, undurchschaubarer und unstrukturierter das Design der Software ist, umso schwerer wird es sein, und entsprechend lange wird es dauern, bis das System geknackt ist. Sobald dieser „Unsicherheitszustand“ bekannt ist, bekommen alle Nutzer über eine in das DRM-System integrierte Zwangs-Update-Funktion ein neues Stück Software, das wieder solange Schutz bietet, bis es ebenfalls geknackt ist u.s.w.

Wir wagen die These, dass je nach Motivation des Angreifers und Wert des Inhalts ein solcher Zyklus mit einer Periode von einigen Monaten oder länger beginnen kann, die Periode wird sich jedoch im Mittel verkürzen und kann nach mehreren erfolgreichen Hacks nur noch einige Tage

oder gar Stunden betragen. Der Grund hierfür liegt in der Tatsache begründet, dass der Vorrat an undurchschaubaren Konzepten und Denkstrukturen, die der Designer der DRM-Software besitzt und nutzen muss, um das Hacken zu erschweren, stets begrenzt ist. Man kann davon ausgehen, dass irgendwann die „guten Ideen“, die das Design verworrener machen, weitgehend erschöpft sein werden.

Folgender Vergleich mit der Sicherheit von Kryptographie verdeutlicht das Problem noch auf andere Weise: In den letzten 100 Jahren wurden höchstens 10–20 grundlegend verschiedene Ideen zum Design von Verschlüsselungsfunktionen vorgestellt, die sich bewährt haben. Diese kleine Zahl muss jedoch nicht erschrecken, da die Sicherheit eines Verschlüsselungsverfahrens nicht von der Geheimhaltung des Algorithmus, sondern vielmehr von dessen Parameter, dem Schlüssel, abhängen soll. Der Schlüsselraum heute sicherer Verfahren enthält aber zwischen 10^{20} und 10^{40} gleichwahrscheinliche Möglichkeiten. In Software, wo der Schlüssel als Teil der Daten innerhalb der Software gespeichert werden muss, kann er zur Sicherheit gegen Ausforschung nichts beitragen. Bei hardwarebasierter Kryptographie ist das grundsätzlich anders, da der Schlüssel das Hardware-Modul nicht verlässt: Die Hardware enthält den Schlüssel *und* den Algorithmus, so dass die Ver- und Entschlüsselung ebenfalls über das Hardware-Modul abläuft.

Den Anbietern von softwarebasierter DRM-Technik ist diese Problematik natürlich bekannt (vgl. die Vorträge von Industrievertretern auf der 2. Konferenz Digital Rights Management vom 29.–30. Januar 2002 in Berlin, http://www.digital-rights-management.de/) und sie versuchen, aus dieser Situation nach Möglichkeit noch das beste Sicherheitsniveau herauszuholen, da momentan aufgrund fehlender Hardwarebausteine in PCs keine andere Möglichkeit existiert.

Zusammenfassend muss gesagt werden, dass reine Softwarelösungen auf Dauer nicht geeignet sind, den Schutz digitaler Inhalte zu gewährleisten. Möglicherweise sind auch die Kosten für die Ausstattung von Geräten (PCs, Audio-, Videoabspielgeräte) mit entsprechenden Hardwarebausteinen momentan noch höher als die Verluste, die durch Piraterie und Verbreitung illegaler Inhalte entstehen.

3.5 Umgehen von Sperren und Filtern

Das Sperren von Internetangeboten (siehe auch Abschnitt 2.4.6) dient hauptsächlich dem Schutz des Endbenutzers. Wünscht er diesen Schutz nicht, hat aber sein Provider entsprechende Vorkehrungen getroffen, kann er sich über eine lokale Sperre leicht hinwegsetzen.

3.5.1 Methoden

Abbildung 3.3 zeigt die Umgehung einer Sperre durch den Client-Rechner, indem der Client auf einen sog. Proxy ausweicht, der innerhalb eines Providers 2 liegt und der den Zugang zu dem Server nicht gesperrt hat. Solange der Provider 1 den Zugang zu Provider 2 nicht ebenfalls sperrt oder Provider 2 nicht seinerseits den Zugang zu dem Server blockiert, gelingt dieses Ausweichen. Eine Sperre ist damit unwirksam, solange nicht alle Provider (weltweit) ebenfalls den Server blockieren.

Auch ein Server ist in der Lage, eine Sperrung zu umgehen, indem er z.B. alle Minuten seine IP-Adresse ändert. Bei Inhalten in Newsgruppen wird einfach ein Inhalt in andere, bisher un-

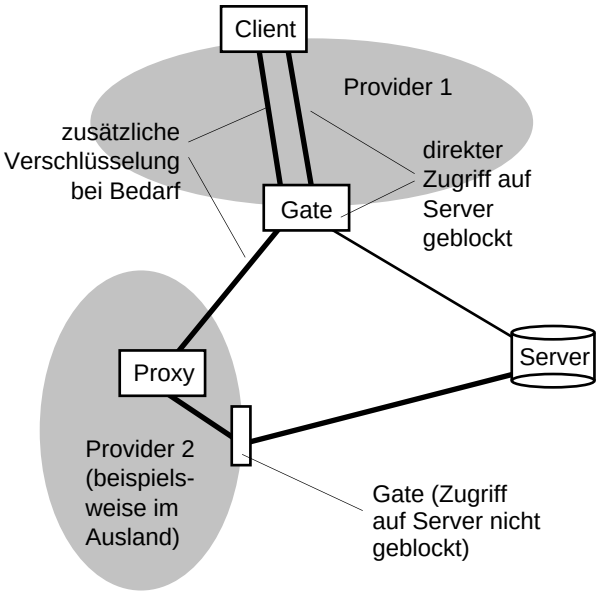

Abbildung 3.3: Ausweichen auf einen fremden Provider überbrückt die Sperre

verdächtige und einwandfreie Newsgruppen „gepostet“. Auch ein Namenswechsel der Newsgruppe bewirkt für einige (kurze) Zeit die ungefilterte Verbreitung von Inhalten. Generell ist es dem Content Provider möglich, falls er sich über eine Sperre hinwegsetzen möchte, sich dynamisch an die Filterkriterien anzupassen. Somit gelingt das Filtern und Sperren von Inhalten bestenfalls auf Zeit.

3.5.2 Konsequenzen

Eine reaktive Sperrung von Inhalten im Internet ist möglich und in vielen Fällen auch zumutbar. Eine proaktive Suche nach rechtswidrigen Inhalten kommt einer Massenüberwachung aller Kommunikation gleich und versagt, falls die Daten verschlüsselt werden. Dies gilt ebenso für Individualkommunikation (z.B. E-Mail) wie für geschlossene Benutzergruppen, die rechtswidrige Inhalte verschlüsselt austauschen.

Eine Sperre äußert sich als „technischer Defekt“. In einem verteilten System wie dem Internet, in dem niemand eine globale Übersicht über den Netzstatus hat, ist für einen Administrator die Einschätzung der Fehlerursache sehr schwer, möglicherweise gar unmöglich. So wird es häufiger zu Fehleinschätzungen (Fehler oder Sperre?) kommen, die eine Administration des Netzes erschweren. Folglich ist eine globale Übersicht über die Sperren notwendig.

Die manuelle Kontrolle aller Inhalte des Internet ist unzumutbar. Hat man ein Angebot als kritisch erkannt und möchte es sperren, beginnt der Wettlauf zwischen Anbieter und Filter, da der Anbieter sich an die Filterkriteren anpassen wird, um die Sperre zu umgehen. Solange ein Anbieter mit seinen rechtswidrigen Inhalten ins Ausland abwandern kann, sind lokale Sperrungen nur ein wenig wirkungsvolles Mittel; internationale Regelungen jedoch können greifen, da sie das Abwandern wirkungslos machen.

3.6 Missbräuchlich verwendbare Werkzeuge

In den folgenden Abschnitten sollen Werkzeuge (Hard- und Software sowie Internetdienste) diskutiert werden, die auch dazu benutzt werden können, um geschützte Inhalte unberechtigt zu vervielfältigen oder Spuren bei illegalen Handlungen zu verwischen, obwohl diese Werkzeuge ursprünglich nicht für diesen Zweck entwickelt wurden.

3.6.1 Kopiervorrichtungen (Grabber, Brenner)

Gemäß der Tabelle 1.2 aus Abschnitt 1.3.3 sollen Dienste, die synchron und online oder asynchron und offline verteilt werden, als klassische Distributionsformen bezeichnet werden. Eines der wesentlichen Merkmale der klassischen Distribution ist die Verteilung exakt gleicher Kopien an alle Konsumenten. Dies hat zur Folge, dass einer illegalen Kopie nicht anzusehen ist, wer die Kopie aus dem Original angefertigt hat und welchen Verteilweg sie genommen hat.

Ein Schutz vor Verbreitung digitaler 1:1-Kopien wurde in der Praxis bisher lediglich dadurch erreicht, dass das Herstellen solcher Kopien zu aufwendig oder zu teuer war. Die technische Entwicklung ermöglicht heute jedoch das preiswerte Anfertigen von Kopien.

Noch vor ein paar Jahren war das Anfertigen einer digitalen Kopie einer Musik-CD teurer als der Kauf der Original-CD. Heute lassen sich auf einer beschreibbaren Compact Disc (CD-R) mit einem handelsüblichen Computer digitale Kopien einer Musik-CD anfertigen. Der Rohling kostet weniger als 1 Euro und das Kopieren dauert maximal etwa 1 Stunde, typisch dürften 10 Minuten sein.

Die gleiche (technische und ökonomische) Situation könnte voraussichtlich in wenigen Jahren mit der Digital Versatile Disk (DVD) eintreten, auf der Videos und andere große Datenmengen gespeichert werden. Allerdings hat man sich bemüht, die Computerindustrie bei der Standardisierung der Kopierschutzmechanismen mit ins Boot zu bekommen, was seinerzeit bei der Festlegung des Audio-CD-Formats noch nicht der Fall war. Deshalb verfügen auch die in PCs eingebauten DVD-Laufwerke über Ländercode-Auswertung (Abschnitt 2.4.2). Besitzen diese PCs ausserdem Grafikkarten mit einer Videoausgabe (TV out, S-Video oder Composite-Signal), muss auch das Macrovision-Kopierschutzsystem (Abschnitt 2.3.1) implementiert sein.

Um die Situation im Musik-CD-Bereich nicht weiter zu verschlimmern, werden neuerdings vereinzelt Musik-CDs in einem Format erzeugt und verkauft, das in CD-ROM-Laufwerken von handelsüblichen PCs nicht problemlos gelesen werden kann. Bei der von Sony angewendeten Technik key2audio [33] werden bestimmte Datenbereiche (hier: das Inhaltsverzeichnis der CD), die nur von Computer-CD-ROM-Laufwerken gelesen werden, mit Daten beschrieben, die das CD-ROM-Laufwerk falsch interpretiert und damit „verwirrt“, so dass es das Abspielen der CD verweigert. Ein Audio-CD-Spieler wird dadurch nicht beeinträchtigt. Andere Verfahren verhindern zwar nicht das Abspielen einer Musik-CD auf einem Computer, sollen jedoch das Kopieren der digitalen Daten durch speziell aufgebrachte Fehler auf der Original-CD verhindern.

Leider sind Techniken wie key2audio völlig ungeeignet, das Anfertigen von Kopien *auf Dauer* zu verhindern, da es sich um schwache Schutzmechanismen handelt, die teilweise nur solange halten, bis jemand ein entsprechendes Auslese- und Kopierprogramm schreibt, mit dem der Schutz umgangen werden kann. Mit key2audio geschützte CDs können beispielsweise mit dem

Programm CloneCD problemlos kopiert werden, berichtete die Computerzeitschrift PC-Welt im Internet (http://www.pcwelt.com/ratgeber/hardware/17678/5.html).

Die Nutzungsqualität privat produzierter Kopien übertrifft derzeit oft sogar die von kommerziell erhältlichen Medien bei weitem. Eine gekaufte Musik-CD beispielsweise enthält ca. 70 Minuten Musik in einer vom Hersteller fest vorgegebenen Zusammenstellung. Eine privat erstellte Kopie dieser Musik auf einem DVD-RAM-Medium mit MPEG-Level-3 komprimierten Audiodaten hat bei vergleichbarer Qualität die fünfzigfache Spieldauer, überlässt dem Ersteller eine freie Auswahl der Zusammenstellung und Abspielreihenfolge, erlaubt die individuelle Ergänzung der Musik mit Zusatzinformationen und Auswahlmenüs. Darüber hinaus können sogar bequemst beim Vervielfältigen oder Abspielen Parameter frei modifiziert werden, die früher die Studiotechniker für alle Hörer fest vorgaben. Zum Beispiel kann die Lautstärkedynamik für bessere Hörbarkeit gegen Hintergrundgeräusche bei Autofahrten reduziert werden.

3.6.2 Peer-to-Peer-Netzwerke (P2P) und öffentliche File-Sharing-Systeme

Das Herstellen und die Re-Distribution (auch: Superdistribution, siehe auch Abbildung 3.4) von legalen wie illegalen Kopien kann heute über Dienste stattfinden, die teilweise darauf spezialisiert sind, bestimmte Medienformen möglichst unkontrollierbar zu verbreiten. Zur Verbreitung können verwendet werden:

- **Private Webpages**, News-Groups, E-Mail, auch wenn diese Dienste nicht spezialisiert sind auf bestimmte Medienformen,
- **Scour** (und Verwandte), ein „shared directory“, das mit komfortablen Suchfunktionen ausgestattet ist und spezialisiert, aber nicht beschränkt ist auf Bilder, Videos und Musikstücke (http://www.scour.com/),
- **Napster** (und Nachkommen), eine zentrale Vermittlungsdatenbank für MP3-Dateien; die Datei wird anschließend direkt zwischen dem Anbieter und Interessenten übermittelt, ohne durch den Napster-Server zu laufen (http://www.napster.com/),
- **Gnutella**, ein dezentralisiertes System, das zum Bereitstellen von beliebigen Inhalten geeignet ist. Bei Gnutella sind sowohl die Vermittlungsdatenbank als auch die Daten dezentralisiert (http://gnutella.wego.com/).

Über diese Dienste konnten Inhalte kostenlos angeboten und abgerufen werden. Die Systeme sind teilweise momentan nicht in Betrieb, da an der Erarbeitung von Geschäftsmodellen und Software für kostenpflichtigen Abruf (dann hoffentlich ausschließlich legal angebotener Inhalte) gearbeitet wird. Die Wiedergeburt von Napster & Co. hat jedoch weniger mit der zwischenzeitlichen Entwicklung besserer Schutzmöglichkeiten zu tun, als mit der Beliebtheit dieser Dienste in vergangenen Tagen. Man erwartet, dass die Nutzer trotzdem zu den ihnen „liebgewordenen“ Diensten zurückkehren werden.

Momentan laufende Systeme sind z.B. MusicCity Morpheus (http://www.musiccity.com/), Audiogalaxy Satellite (http://www.audiogalaxy.com/), BearShare (http://www.bearshare.com/) und iMesh (http://www.imesh.com/).

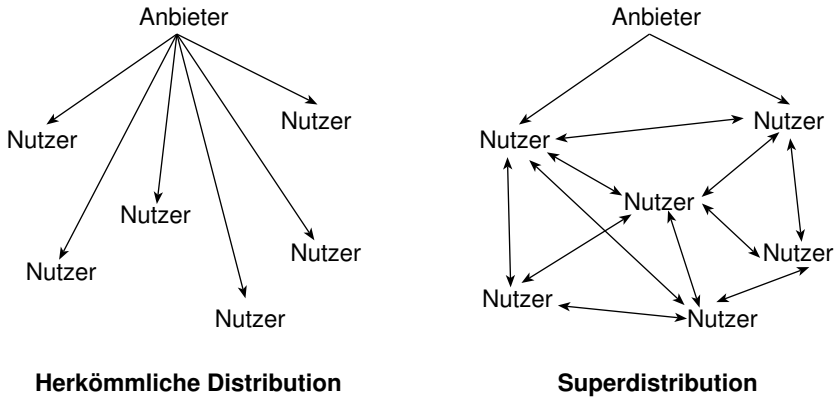

Abbildung 3.4: Superdistribution von Inhalten

Dabei wurde die Superdistribution nicht erst mit den Peer-to-Peer-Lösungen erfunden: Bereits Anfang der 80er Jahre wurde von dem Japaner Ryoichi Mori ein DRM-Konzept zur Verteilung von Inhalten entwickelt, bei dem keine Gebühr für den Erwerb, sondern für die Nutzung von Inhalten entstehen soll. Damit koppelt dieses Distributionskonzept die Vergütung von der Distribution der Inhalte ab [4, S.127ff].

Die illegale synchrone Re-Distribution von Rundfunk und Fernsehen, d.h. das unberechtigte „Ausstrahlen“ z.B. im Internet dürfte derzeit in den meisten Fällen noch am Mangel an technischer Ausstattung scheitern. Allerdings werden die Rechner und Internetverbindungen immer schneller. Software, mit der Jedermann seine eigene Internet-Radiostation betreiben kann, ist bereits am Markt. Beispiel Shoutcast: „SHOUTcast is Nullsoft’s Winamp-based distributed streaming audio system. Now you can listen to live streaming audio, and even broadcast your own SHOUTcast station from the comfort of your regular Internet connection.“ (http://www.shoutcast.com/).

Solche Programme sind sowohl für live- als auch für on-demand MP3 Internet Broadcast geeignet. Natürlich könnten diese Stationen auch mit fremden Inhalten gespeist werden.

3.6.3 Anonyme und unbeobachtbare Kommunikationsdienste

Die auf der Netzwerkebene des Internet vorhandene Adressierungsinformation kann verwendet werden, um den Anbieter bzw. Konsumenten von Inhalten zu verfolgen (siehe auch Abschnitt 2.4.5). Zeropaid (http://www.zeropaid.com/busted) betreibt beispielsweise einen Gnutella-Server, der die Interessenten von Kinderpornographie mit eindeutigen Dateinamen locken soll. Hinter den Dateien verbergen sich allerdings nicht die erwarteten Inhalte, jedoch erfährt Zeropaid die IP-Adresse des an dem Material Interessierten, um ihm anschließend möglichst das Handwerk zu legen.

Zukünftig könnten völlig legal angebotene Anonymisierer allerdings jegliche Verfolgung verhindern. Beispiele:

- **Anonymizer** (http://www.anonymizer.com/) ist ein anonymisierender Proxy-Server. Das bedeutet, der Abruf einer Webseite erfolgt nicht direkt durch den Benutzer, sondern stellvertretend durch den Anonymisierer. Der Betreiber des Webservers und dessen Log-Files haben somit keine verwertbaren Spuren zur Rückverfolgung des Piraten.

- **Freenet** (http://freenet.sourceforge.net/) ist ein dezentralisiertes System, bei dem sich Inhalte, sofern sie von anderen Nutzern tatsächlich abgerufen werden, nicht einfach löschen lassen, da sie sich durch eine spezielle Caching-Technik im „Freenet“ ausbreiten. Der Dienst wurde entwickelt, um free speech im Internet zu realisieren, d.h. unter anderem die Möglichkeit, unzensiert und anonym im Internet zu publizieren.

- **AN.ON** (http://anon.inf.tu-dresden.de/) ist ein eigenes Forschungsprojekt, welches ebenfalls belegt, dass die Anonymisierung von Internetzugriffen zwar aufwendig, aber technisch möglich ist. Zum unbeobachtbaren Surfen im Web ist das System JAP verfügbar.

Bezüglich des technischen Schutzes des Urheberrechtes sind Forderungen nach einem Verbot von privater, anonymer und unbeobachtbarer Kommunikation lediglich das Resultat unzureichender Schutzmechanismen im Vorfeld. Anstatt die Wirkung zu bekämpfen, sollte besser bei den technischen Ursachen begonnen werden, d.h. das leichte und unkontrollierte bzw. illegale Kopieren und Verbreiten von Inhalten muss erschwert oder von neuen Geschäftsmodellen und Diensten qualitativ und bzgl. Bequemlichkeit übertroffen werden.

3.6.4 Trojanische Pferde, Computerviren u. ä.

Viren, Würmer und Trojanische Pferde können nicht nur die Integrität und Verfügbarkeit von Daten und Programmen verletzen, sondern alle Schutzziele, also auch die Vertraulichkeit von Daten. Ein **Computervirus** ist ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine sog. **Schadensfunktion** ausführt. Ein **Wurm** ist ein ausführbares Programm, das sich über Computernetze verbreitet und ggf. eine Schadensfunktion ausführt. Ein **Trojanisches Pferd** ist ein Computerprogramm, das neben einer bekannten (vom Anwender gewünschten) Funktion eine (nicht gewünschte) Schadensfunktion ausführt.

Dies bedeutet, dass ein Angreifer z.B. einen Virus oder ein Trojanisches Pferd schreiben könnte, dessen Aufgabe es ist, fremde Festplatten, Computer und Computernetze nach urheberrechtlich geschütztem Material abzusuchen.

- Ein Pirat könnte so unberechtigt an die legal erworbenen Inhalte, Schlüssel etc. eines Anderen kommen und die ihn interessierenden Daten „absaugen“.

- Ein Verfolger könnte mit dieser Methode versuchen, illegal vorhandes Material aufzuspüren und entsprechende Maßnahmen (z.B. Löschen, Strafverfolgung) einleiten.

Beides ist unter normalen Umständen illegal. Technisch gesehen beruht die Angriffsmöglichkeit über trojanische Pferde und Computerviren auf einer fehlenden (z.B. in DOS, Windows 95/98/ME, MacOS bis Version 9) oder schlecht eingesetzten Zugriffskontrolle. Insofern ließe sich zumindest die Virenproblematik durch entsprechend stärkere Beachtung und sichere Vor-Konfiguration von Zugriffskontrollmechanismen durch die Hersteller von Betriebssystemen halbwegs in den Griff bekommen. Gegen trojanische Pferde hilft, sobald man die Virenproblematik zufriedenstellend gelöst hat, trotzdem nur der sensible und bewußte Umgang der Benutzer mit ausführbaren fremden Inhalten: Da man einem trojanischen Pferd die Hinterlist zunächst nicht ansieht, muss man der Korrektheit der Funktionalität (hier: Ausschließlichkeit der dokumentierten Funktionalität) vertrauen.

4 Konsequenzen und Sekundäreffekte

Für den Verbraucher bzw. Konsumenten von Inhalten entstehend durch die technisch unterstützte Sicherung des Urheberrechtes Konsequenzen und Sekundäreffekte, auf die in den folgenden Abschnitten eingegangen wird. Dies betrifft insbesondere die informationelle Selbstbestimmung der Konsumenten und den Verbraucherschutz.

4.1 Sicherung der informationellen Selbstbestimmung

In seinem sehr gut geschriebenen Überblickpapier „Golden Times for Digital Rights Management?“ nennt Tomas Sander im Kapitel „2.1 Dependable Digital Rights and Portability“ folgendes Fernziel: „The ultimate challenge is to bind digital rights to a person, and not to a (set of) device(s).“ Dies macht das Spannungsverhältnis zwischen informationeller Selbstbestimmung und dem effektiven Schutz digitaler Inhalte deutlich.

4.1.1 Unbeobachtbarkeit und Anonymität

Informationelle Selbstbestimmung der Nutzer digitaler Inhalte bedeutet, dass sie so weit wie möglich autonom und frei bestimmen,

- wem sie ihre Nutzung digitaler Inhalte wann und unter welchen Umständen wie weit offenbaren (Unbeobachtbarkeit der Nutzung) und
- wem sie ihren Erwerb digitaler Inhalte zur Kenntnis gelangen lassen (Anonymität des Erwerbs).

Die heute weitestgehend gegebene Unbeobachtbarkeit der Nutzung digitaler Inhalte wird untergraben, wenn Inhalteanbieter oder ihre Vertriebspartner

- zum Zwecke der Einzelnutzungsabrechnung (Pay-per-use) detaillierte Abrechnungen vom Endsystem des Nutzers erhalten oder gar
- zum Zwecke der Freischaltung jeder einzelnen Nutzung eine Anfrage erhalten, um die entsprechende Autorisierungsnachricht an das Endsystem des Nutzers zu schicken, ohne die dieses den Inhalt nicht nutzen lässt.

Maßnahmen, die die Untergrabung der Unbeobachtbarkeit der Nutzung begrenzen, sind wenig detaillierte Einzelnutzungsabrechnungen, die in keinem Fall den genauen Nutzungszeitpunkt

enthalten sollten sowie möglichst wenige Angaben über die im Detail genutzten Inhalte. Anzustreben ist, dass die Einzelnutzungsabrechnung nur die für den Abrechnungszeitraum insgesamt zu zahlenden Entgelte als eine Summe ausweist. Aus Sicht der Unbeobachtbarkeit der Nutzung und damit des informationellen Selbstbestimmungsrechts extrem bedenklich sind Systemgestaltungen, die für jede Einzelnutzung Autorisierungsnachrichten erfordern, da dann der zeitliche Ablauf der Nutzung durch den Nutzer dem Inhalteanbieter oder seinem Vertriebspartner offenbar wird. Hier bliebe dann nur noch die Möglichkeit, eine anonyme Nutzung zuzulassen.

Der heute weitgehend gegebene anonyme Kauf digitaler Inhalte wird untergraben, wenn Inhalteanbieter oder ihre Vertriebspartner

- Käufer oder
- deren mit einer Identität versehene Geräte

identifizieren.

Hierbei ist nicht nur zu betrachten, welche Identifikation der Inhalteanbieter oder sein Vertriebspartner vornimmt, sondern auch, welche mittelbare Identifikation etwa durch das verwendete Zahlungssystem (z.B. Kreditkarten) erfolgt.

Beobachtungsmöglichkeiten über Seriennummern von Geräten sind bereits seit langem Realität. So verfügen beispielsweise Digital-Audio-Recorder, die mit dem Serial Copy Management System (SCMS, siehe Abschnitt 2.4.1) ausgestattet sind, über einen Recorder Unique Identifier (RID), ein 97 Bit langer Code, bestehend aus einem Herstellercode, einer Typnummer und einer eindeutigen Seriennummer des eingebauten Laufwerks. Jeder mit einem solchen Recorder aufgenommene Inhalt enthält alle 100 Datenblöcke des Audio-Datenstroms diesen RID. Der RID wurde eingeführt, um die Quelle unautorisierter Kopien besser verfolg- und identifizierbar zu machen.

Sind die verwendeten Maßnahmen zum Schutz der digitalen Inhalte technisch nicht sicher, was zumindest in der überschaubaren Zukunft der Fall sein wird, so arbeiten alle Möglichkeiten, den Nutzern Unbeobachtbarkeit zu gewähren bzw. den Käufern Anonymität, klar gegen die im Interesse der Inhalteanbieter anzustrebende Risikobegrenzung durch Beobachtbarkeit und Nachverfolgbarkeit der Ausnutzung von Sicherheitslücken.

4.1.2 Fälschliche Beschuldigung

Um bei Weiterverbreitung digitaler Inhalte „beweisen“ zu können, wer sie weiterverbreitet hat, wird die Identität des Käufers bzw. Nutzers in den digitalen Inhalt eingebettet (Fingerprinting). Neben der bereits bei der Beschreibung von Fingerprinting in Abschnitt 2.3.3 dargelegten Unsicherheit – sie ist noch größer und grundlegender als bei Watermarking – aller bisher bekannten Verfahren (Fingerprints können leicht entfernt werden), bieten Fingerprints noch zwei weitere Unsicherheiten. Diese können leicht zu fälschlichen Beschuldigungen führen:

- Derjenige, der den Fingerprint in den digitalen Inhalt einbringt, kennt exakt die gleiche Fassung des Inhalts wie derjenige, der den mit dem Fingerprint versehenen Inhalt erhält. Wird der mit dem Fingerprint versehene Inhalt an unbefugter Stelle aufgefunden, kann die undichte Stelle bei jedem von beiden liegen. Ein Beweis im Sinne des Zivilrechtes kann mit diesem Hilfsmittel allein also nicht geschaffen werden.

- Dass der mit einem Fingerprint versehene Inhalt an unbefugter Stelle aufgefunden wird, muss nicht auf böswillige Absicht oder auch nur Billigung eines der beiden Beteiligten beruhen. Heutige IT-Systeme sind größtenteils so komplex und unsicher, dass auch der Systembetreiber sich ihrer Funktion nicht sicher sein kann. Dies gilt insbesondere für alle IT-Systeme, wo Software dynamisch nachgeladen werden kann.

Aus den genannten Gründen müssen „Beweise“ für Urheberrechtsverletzungen, die Systeme zum Schutz digitaler Inhalte liefern, mit einer gehörigen Portion Skepsis betrachtet werden.

4.2 Langfristige Sicherung des Verbraucherschutzes

Die Akzeptanz von Schutzsystemen durch den Endverbraucher hängt auch davon ab, ob seine Interessen langfristig gewahrt bleiben. Die beiden folgenden Abschnitte betrachten diesen Aspekt für die Archivierung von Kulturgütern und die Situation, wenn die immer schneller werdenden Technologiezyklen den Wunsch des Verbrauchers nach Anpassung legal erworbener Inhalte an neue Technik entstehen lassen.

4.2.1 Kopierschutz vs. Archivierbarkeit von Kulturgütern

Hauptaufgabe von öffentlichen Bibliotheken ist es, den Kulturbesitz einer Gesellschaft zu erhalten, zu erweitern und möglichst vielen Benutzern zugänglich zu machen [40, 3]. Um diese Aufgabe zu vereinfachen, ist in vielen Ländern das Urheberrecht an eine Abgabepflicht von Belegexemplaren gebunden. Verleger geistiger Werke sind beispielsweise in Großbritannien verpflichtet, ein Belegexemplar an die British Library zu senden, und fünf weitere nationale Copyright-Bibliotheken haben das Recht, kostenlos ein Exemplar anzufordern. Der langfristige Erhalt dieses Bestandes über mehrere Jahrhunderte erfordert nicht nur die sorgfältige Aufbewahrung und Pflege, sondern auch die Überführung in andere, besser archivierbare Medien. So laufen derzeit etwa in zahlreichen Nationalbibliotheken große Projekte, um signifikante Teile des Buchbestandes einzuscannen, also in eine digitale und damit problemlos beliebig oft verlustfrei kopierbare Form zu wandeln. Die Abgabepflicht für Belegexemplare beschränkt sich derzeit oft noch auf gedruckte Werke, aber eine Erweiterung auf elektronische Werke inklusive Datenbanken, Computersoftware- und Spiele, etc. wird derzeit erwogen. Das Britische National Sound Archive verfügt beispielsweise bereits über eine Million privater und kommerzieller Tonträger [40].

Diese Arbeit zum langfristigen Erhalt von geistigen Werken könnte aber in absehbarer Zeit durch hocheffektive Kopierschutzmechanismen in elektronischen Medien gefährdet werden. Sicherlich werden für Werke, die in den Jahren nach der Erstveröffentlichung Popularität genießen, die Verleger selbst am Erhalt und der kontinuierlichen kommerziellen Verfügbarkeit des Produktes interessiert sein. Ein guter und langfristig wertvoller Bibliotheksbestand ist jedoch weniger nach dem aktuellen Interesse der Benutzer für den Bestand zu beurteilen, sondern danach, ob die Bibliothek auch in der Lage ist, in fernerer Zukunft noch ein umfassendes und unvoreingenommenes Abbild des gesamten kulturellen Geschehens über verschiedene Epochen hinweg zu erhalten, inklusive möglichst vieler auf Anhieb vielleicht weniger erfolgreicher Werke, von denen einige eventuell erst nach Jahrzehnten oder Jahrhunderten auf Interesse stoßen.

„Wie jedes Eigentum unterliegt auch das geistige Eigentum gewissen Schranken im Rahmen der Sozialpflichtigkeit. Ein der Öffentlichkeit – auf welche Weise auch immer – zugänglich gemachtes Werk ist durch seine Veröffentlichung Teil der Gesellschaft geworden – wie das Bundesverfassungsgericht formuliert hat. Es sollte ihr zur ungehinderten Nutzung zur Verfügung stehen.“ [3].

Bibliotheken kämpfen bereits jetzt mit einem enormen Erhaltungsproblem, das den Bestand fast aller gedruckter Werke der letzten 150 Jahre bedroht. Während sorgfältig hergestellte klösterliche Schriften aus dem Mittelalter noch heute in hervorragendem Zustand erhalten sind, so hat ein Großteil der im 20. Jahrhundert gedruckten Literatur nur eine Lebenserwartung von 50–80 Jahren [51]. Da sich seit etwa 1840 in der Papierherstellung eine kostengünstige Harz-Alaun-Leimung durchgesetzt hat, enthält modernes Papier Schwefelsäure und säurebildende Substanzen, die im Zusammenwirken mit der allgegenwärtigen Luftfeuchte die Zellulosefasern des Papiers im Lauf der Jahre brüchig werden lassen. Es wurde beispielsweise in den USA geschätzt, dass dort 70–90 Prozent der Dokumente vom Papierzerfall betroffen sind und bereits 15–30 Prozent heute nicht mehr benutzbar sind. Eine Untersuchung des Deutschen Bibliotheksinstituts ergab, dass in Deutschland in wissenschaftlichen Bibliotheken etwa 60 Millionen Bücher und in Archiven etwa 350 km Regallänge vom Zerfall bedroht oder schon betroffen sind. Ohne entsprechende Maßnahmen wird damit das geistige Erbe der Menschheit des 20. Jahrhunderts nicht für die Nachwelt erhalten bleiben.

Mit dem breiten Einsatz hocheffektiver Kopierschutztechnik im Publikationswesen der Zukunft droht Bibliotheken nichts anderes als eine Wiederholung des aktuellen Säureproblems mit Druckmedien im nächsten Jahrhundert für digital gespeicherte Werke.

Mit ständig steigenden Integrationsdichten digitaler Datenträger reduziert sich auch immer weiter die physikalische Redundanz der Datenrepräsentation und damit auch die langfristige Lesbarkeitsdauer des Mediums.

Kopierschutzmechanismen könnten künftig Bibliotheken nicht nur an der Übertragung alter Werke auf neuere, zeitgenössische, kompaktere und preiswertere Datenträger hindern und damit ein enormes Kostensparpotential für Bibliotheken und Archive eliminieren. Sie verhindern notwendigerweise auch die Anfertigung von Kopien für den Fernverleih und die Rettung des Datenbestandes am Ende der Haltbarkeit des Mediums.

4.2.2 Legitimes Kopieren und Reverse Engineering

Gleichwertig neben dem Interesse der Verleger geistiger Werke daran, eine gewinnschädigende unlautere Weitergabe an andere Benutzer zu vereiteln, bestehen auf Seiten vieler Kunden eine Reihe von durchaus legitime Bedenken gegen den Einsatz umfassender Kopierschutzmechanismen, vergleichbar mit den Sorgen der Archive und Bibliotheken.

Digitale Speichertechnologien (derzeit hauptsächlich magnetische, optische, und magnetooptische Plattenspeicher als austauschbare Medien oder fest gekapselte Laufwerke, sowie Halbleiterspeicher) unterliegen derzeit und auf absehbare Zeit hinaus einem exponentiellen Leistungswachstum in Merkmalen wie etwa Kapazität, Geschwindigkeit, Gewicht, Energieverbrauch, und Geräuschentwicklung. Schnelle Technologiezyklen machen Medien oft innerhalb von weniger als einem Jahrzehnt obsolet, und Kunden sind daher daran interessiert, erworbene geistige Werke selbstständig auf modernere Medien übertragen zu können. In gewisser Weise wären unflexible Formen von Kopierschutzmechanismen, die diesen Konsumentenanforderungen nicht

nachkommen, in etwa vergleichbar mit beispielsweise einer hypothetischen Buchdrucktechnologie, bei welcher der Kunde nur mittels seiner zum Kaufzeitpunkt aktuellen Lesebrille den Text lesen kann. Auch wenn zum Erwerbszeitpunkt dem Kunden der erkaufte Nachteil nicht bewusst wird, so sind die Nutzungsrechte doch nach einiger Zeit erheblich eingeschränkt.

Kontinuierlicher Gebrauch geht bei allen physikalischen Medien mit der Gefahr einher, dass die Medien durch erhöhte Temperatur und Erschütterungen sowie mechanischen Abrieb schneller altern als die gewünschte Nutzbarkeitsdauer des Produktes, die sich bei vererbten Bibliotheken oft über mehrere Generationen hin erstrecken kann, dies erlaubt. Moderne Speichermedien sind oft sehr sensibel gegenüber ungeeigneten Umwelteinflüssen und es besteht ständig die Gefahr, dass durch einen Unfall oder kurzfristige unsachgemäße Handhabung die Lesbarkeit der Daten beeinträchtigt wird. Im Bereich von Computersoftware herrscht daher ein seit langem akzeptiertes Gewohnheitsrecht, welches es Kunden erlaubt, sich Sicherheitskopien der erworbenen Medien zu erstellen.

Manche der zuvor genannten Bedenken wie etwa die Übertragbarkeit auf modernere Medien ließen sich gegebenenfalls durch geeignete „Online-Authentisierungstechniken“ praktikabel begegnen, aber um diese nutzen zu können, ist der Kunde darauf angewiesen, dass der Hersteller auch nach vielen Jahren noch die Möglichkeit bietet, Nutzungslizenzen von einem Medium oder Abspielgerät auf ein anderes zu übertragen. Dies ist insbesondere problematisch, wenn der Hersteller inzwischen das Geschäft aufgegeben hat.

Im Falle von Computersoftware kommt als weitere Kundensorge hinzu, dass ein umfassender Kopierschutz auch eine Inspektion der ausgeführten Maschineninstruktionen vereiteln würde, was erheblich die Möglichkeiten der Kunden reduzieren würde, das Produkt im Rahmen von Produkthaftungsansprüchen oder Patentlizenzforderungen eingehend zu untersuchen.

4.3 Fazit und offene Fragen

Momentan sind die verfügbaren Systeme zum Schutz von Inhalten systematisch unsicher.

Die existierenden Systeme haben trotz (oder gerade wegen) ihrer Unsicherheit Sekundäreffekte für Datenschutz und Verbraucherschutz, indem sie die Beobachtbarkeit und das Profiling der Nutzer ermöglichen oder wenigstens nicht verhindern. Weiterhin wird die freie und uneingeschränkte Nutzung von legal erworbenen Inhalten verhindert.

Wenn die existierenden Systeme tatsächlich sicher wären, bzw. wenn irgendwann sichere Systeme entwickelt und am Markt sein sollten, dann hätten sie auch Auswirkungen auf die Archivierbarkeit und die zeitlose Verfügbarkeit der über sie gesicherten Inhalte. Hier sollte man ggf. den Weg gehen, öffentliche Archive mit Kopien der Inhalte zu versorgen, die auch tatsächlich archivierbar und (zeitlos) nutzbar sind.

Die stärkere Verbreitung von DRM-Technik wirft im übrigen einige Fragen auf, die aus unserer Sicht bisher noch nicht ausreichend in der Öffentlichkeit diskutiert sind:

- Sind die Endverbraucher ausreichend geschützt und wer wird zukünftig ihre Rechte wahrnehmen?
- Brauchen wir möglicherweise für die Zukunft neue „Codes of Conduct“ für den Umgang mit Forschungsergebnissen über die Unsicherheit von Sicherungssystemen generell, da bereits heute Gesetze existieren, die die Freiheit wissenschaftlicher Arbeit beeinflussen?

- Welche Implikationen haben DRM-Systeme für die wissenschaftliche Arbeit? Das (wachsende) Angebot an momentan kostenlos und frei abrufbaren wissenschaftlichen Publikationen im Internet könnte mit der Einführung von DRM-Systemen schlagartig sein Ende finden.
- Im engeren Sinn stellt sich deshalb die regulatorische Frage, ob und ggf. wer den Zugang und die Nutzung von Information kontrollieren darf. Keinesfalls sollte Technik hier den Einscheidungsrahmen einschränken.

5 Zusammenfassung

In den vorangegangenen Kapiteln wurden Verfahren zum Schutz digitaler Inhalte vorgestellt und bewertet. Die dargestellten Angriffsmethoden machen deutlich, dass die Verfahren in der Praxis keinen perfekten Schutz gewährleisten können.

Nachfolgend sollen die Problematik, die Lösungsansätze und der Stand der Technik noch einmal kurz zusammengefasst werden.

Generelles Schutzziel von DRM-Systemen

DRM-Systeme sollen den Rechteinhabern einen sicheren Vertrieb, differenzierte Rechteverwaltung und eine Kontrolle der Nutzung digitaler Inhalte ermöglichen.

Das Paradoxe an DRM-Systemen ist, dass man einem Kunden einen Inhalt in einer bestimmten Weise zugänglich machen will und muss, ihn gleichzeitig aber daran hindern möchte, *alles* (= beliebiges) damit tun zu können. Sichere Technik, die einem Kunden erlaubte Nutzungsmöglichkeiten einräumt und unerlaubte technisch verhindert oder wenigstens erschwert, ist dabei nur ein Baustein eines DRM-Systems.

Ineinandergreifen von Technik und Recht

Insgesamt erstreckt sich der Schutz nach [4, S.263] über drei Ebenen, die ineinander greifen: Neben

- **Technik**, die ihrerseits durch einen rechtlichen Umgehungsschutz geschützt werden kann, tragen noch
- **Nutzungsverträge** zwischen Kunden und Anbietern, die ihrerseits schützbar sind durch Technik sowie diese wiederum durch den rechtlichen Umgehungsschutz sowie
- **Technologie-Lizenzverträge**

zum Schutz bei (siehe auch Abbildung 5.1). Dieses Ineinandergreifen soll bewirken, dass bei Versagen einer Ebene hoffentlich die nächste einspringt, um die Rechteinhaber zu schützen.

Systematik

Aus technischer Sicht, die ja Gegenstand der vorliegenden Studie ist, stellt sich die Situation folgendermaßen dar. Um das oben formulierte Schutzziel zu erreichen, benötigt man einen

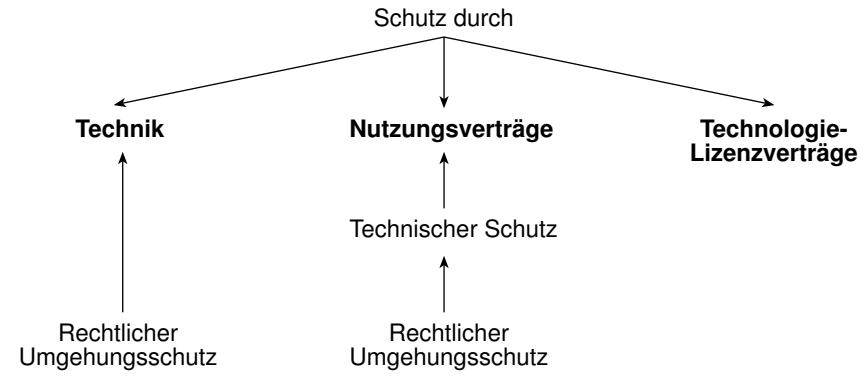

Abbildung 5.1: Unterschiedliche Schutzmechanismen in DRM-Systemen nach [4]

geschützten Bereich GB im Verfügungsbereich VB des Kunden. Dieser GB schützt den Rechteinhaber vor dem Kunden. Daraus folgt, dass GB für den Kunden nicht voll zugänglich sein darf, d.h. GB muss ausforschungssicher gegenüber dem Kunden sein. Diese Forderung entspricht exakt der Forderung, die beispielsweise an Telefon-Wertkarten gestellt werden. Hinzu kommt noch, dass der Inhalt, der dem Kunden zugänglich sein soll, in einer Repräsentation ausgegeben werden muss, die vom Kunden entweder nicht ohne großen Aufwand vervielfältigt werden kann oder den Käufer identifizier- und verfolgbare Informationen eingebettet haben muss, die vom Kunden nicht ohne weiteres entfernbar sind.

Informatischer Ansatz

Für die Analyse von Sicherheitseigenschaften ist die Ausführungs-Schichtenstruktur der beteiligten IT-Systeme grundlegend: Hierbei führt die Schicht i die Objekte der Schicht $i+1$ aus, wobei die Objekte der Schicht i wiederum durch Schicht $i-1$ ausgeführt werden können. Typische Ausführungs-Schichtenstrukturen heutiger IT-Systeme sind (siehe Abbildung 5.2): Die Hardware (Schicht 1: ICs, Leiterbahnen, Fest- und Wechselplatten, u.a. Bauteile angeordnet in Baugruppen, z.B. Prozessor, Arbeitspeicher, Netzwerk-, Audio- und Videokarten, etc.) führt die Systemsoftware (Schicht 2: Betriebssystem, Treiberprogramme etc.) direkt aus. Hardware und Systemsoftware zusammen führen Anwendungssoftware (Schicht 3: Textverarbeitung, Audio-Player, Video-Player, etc.) aus. Die Anwendungssoftware schließlich führt Text(verarbeitung) aus, spielt Tondateien, zeigt Videosequenzen, etc., d.h. führt die Objekte der Ebene 4 aus.

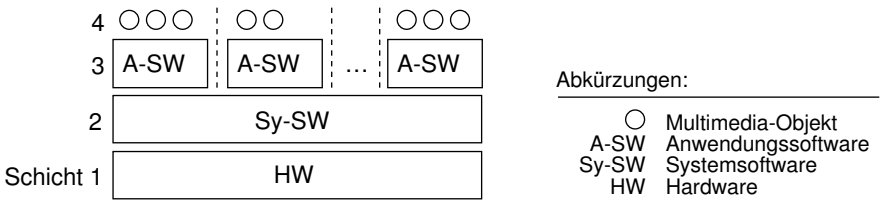

Abbildung 5.2: Ausführungs-Schichtenstruktur

Je nach Anbieter ist der zu schützende Inhalt unterschiedlich: Hardwarehersteller sehen ihre Bauteile als Content, Ersteller der Systemsoftware sehen Systemsoftware als zu schützen-

den Inhalt, Ersteller der Anwendungssoftware sehen beispielsweise Textverarbeitungssoftware, Audio- und Video-Player-Software als Inhalt und Künstler sowie Medienagenturen sehen Tondateien, Videosequenzen etc. als Inhalt.

Grundlegend gilt nun: Ein Schutz der Objekte der Schicht *i* vor den Objekten der darunterliegenden Schichten ist nicht effizient möglich, denn diese müssen die Objekte der Schicht *i* ja ausführen und zumindest insoweit elementar hantieren und „verstehen".

Schutz einer Tondatei vor Missbrauch erfordert Schutz des Audio-Players vor Manipulation. Der Schutz des Audio-Players erfordert wiederum Schutz der Systemsoftware vor Zweckentfremdung und dies schließlich wiederum Schutz der Hardware vor Manipulation — alles jeweils natürlich bezogen auf das konkrete IT-System, auf dem die Tondatei legitimerweise gespielt werden soll.

Bewertung

Im Kapitel 2 wurden Techniken zum Schutz digitaler Inhalte beschrieben. In Tabelle 5.1 werden die Mechanismen noch einmal zusammenfassend dargestellt. In Kapitel 3 wurden die Schwächen von und Angriffsmöglichkeiten auf die Mechanismen vorgestellt.

Man kann davon ausgehen, dass DRM-Systeme zukünftig auch eingesetzt werden, um Hardware- und Softwareplattformen technisch und vertraglich abzusichern, d.h. DRM-Systeme könnten zu einem festen Bestandteil der IT-Infrastruktur auch in Bereichen werden, in denen es nicht nur um mediale Inhalte geht. Die Technik von DRM-Systemen stützt sich im wesentlichen auf grundsätzliche IT-Sicherheitstechniken und ist insofern geeignet, nicht nur multimediale Inhalte, sondern auch beispielsweise Software zu schützen. Insofern deckt diese Studie jede momentan mögliche Form von „Inhalt" und alle derzeit üblichen Distributionsformen (z.B. Online-Dienste und Online-Übertragung, Software-Verteilung und Datenträgeraustausch) ab.

Versuche, den Schutz von Inhalten ausschließlich in Software zu realisieren, sind nahezu hoffnungslos. Dies zeigen die Erfahrungen beim Kopierschutz im Softwarebereich. Für wertvolle Software werden deshalb auch dort Hardwaresysteme (Dongles) eingesetzt.

Verfahren in oder zumindest unter Verwendung von Hardware gewährleisten begrenzten Schutz, da das Knacken der Hardware meist aufwendiger ist. Auch diese Verfahren sind weit entfernt von perfekter Sicherheit.

Da insbesondere die Verfahren, die das Kopieren von Inhalten *verhindern* sollen, nur wenig Sicherheit bieten, wächst die Nachfrage nach Verfahren, die das Kopieren und verbreiten erkennbar und verfolgbar machen. Dies ist auch insofern verständlich, dass Inhalte auch angezeigt bzw. abgespielt werden müssen, d.h. der Schutz sich auch auf die Ausgabekomponente erstrecken müsste, wo die Inhalte hochqualitativ (meist sogar digital) zur Verfügung stehen sollen.

Ausblick

Kriminelle Inhalte ebenso wie die kriminelle Verbreitung von Inhalten im Internet können, wie auch in anderen Medien, nicht einfach toleriert werden. Sie müssen in allen Medien angemessen bekämpft und möglichst verhindert werden. Alle Wege zur Bekämpfung müssen allerdings die Grundentscheidung zwischen Freiheit und Kontrolle treffen. Es gibt neben kulturellen (siehe

Absch.	Schutzsystem/ Technik	Schutzprinzip/ techn. Basis	Was wird bewirkt bzw. verhindert?	Bemerkungen
Präventive Verfahren				
— Verfahren basierend auf physischem Schutz, z.B. in Hardware (HW)				
2.2.3	Dongles	phys. HW-Schutz	verhindert unberechtigte Nutzung von Software	sicher, solange Dongle nicht kopierbar, obwohl Kopieren der Software möglich
2.2.3	Physisch gekapselte (Player)-HW	phys. HW-Schutz	verhindert Abgreifen des digitalen (ggf. entschlüsselten) Medienstroms	mit Aufwand gut, aber nicht perfekt möglich
2.4.3	Inkompatible Formate, Fehlerstellen auf physischem Medium	phys. HW-Schutz, Anbringen eines Sondersignals	verhindert Kopieren durch Aufbringen nicht kopierbarer Stellen auf phys. Medium	sicher, solange keine geeigneten Lese-/Schreibgeräte existieren, meist jedoch gebrochen
— Verfahren basierend auf Software-(SW)-Schutz				
2.2.4	Sandbox	Einkapselung fremder SW	schützt vor bösartiger fremder SW	kein Schutz vor der eigenen Ausführungsumgebung (lokaler PC und dessen Benutzer)
2.4.1	SW-Codes	Geheimhaltung des Codes	verhindert unberechtigte Nutzung, Kopieren möglich	schwacher Schutz, da Codes leicht weitergegeben werden können, meist durch Security-by-obscurity realisiert
3.4.3	DRM-Software	Security-by-obscurity	soll unberechtigte Nutzung des Inhalts verhindern	leicht knackbar, deshalb meist mit einer Zwangs-Update-Funktion ausgestattet, um sicheren Zustand zeitweise wieder herzustellen
— Verfahren zur Absicherung des Distributionsweges				
2.2.2	Verschlüsse-lung	Geheimhaltung eines Schlüssels, Kryptographie	soll unberechtigte Nutzung verhindern und unberechtigtes Kopieren des entschlüsselten Inhalts verhindern, Kopieren des Verschlüsselten leicht	Verhindern der Weitergabe des Schlüssels wie auch des Entschlüsselten ist essentiell, setzt für sichere Anwendung physische Kapselung der Entschlüsselung *und* Digital-Analog-Wandlung voraus
2.3.2	Watermarking	Einbringen eines nicht entfernbaren Sondersignals	soll Wiedererkennung des markierten Inhalts bewirken	Sondersignal kann beliebige Information (z.B. über den Urheber) tragen, Kopieren des markierten Inhalts möglich
2.3.3	Fingerprinting, Traitor Tracing	Kryptographie	bewirkt die Rückverfolgung illegaler Kopien zum legalen Käufer, Kopieren des markierten Inhalts möglich	setzt voraus, dass Inhalte nicht gegen den Willen (oder ohne das Wissen) des legalen Käufers mit Hackermethoden kopiert werden können, sonst fälschliche Beschuldigung
— Codierung mittels Metadaten				
2.4.1	Codes ohne Sicherung	Anbringen eines Kodes	soll Kopieren über mehrere Generationen erschweren	sehr schwacher Schutz, da Codes völlig ungesichert sind und verändert werden können
2.4.2	Regionale Codierung	Anbringen eines Kodes, Verschlüsse-lung des Inhalts	künstliche Marktseparation	Wirkungsvoll, solange Player-Laufwerke noch teuer sind
Reaktive Verfahren				
2.4.5	Aufspüren illegaler Kopien	Inhaltsbasierte Analyse	Rückverfolgung zum Verursacher	zusammen mit Fingerprinting wirkungsvoller
2.4.6	Filter/Sperren	Blockieren des Zugangs	soll den Abruf illegaler Inhalte verhindern	kann meist leicht umgangen werden

Tabelle 5.1: Zusammenfassung der Mechanismen

Abschnitt 4) vor allen Dingen auch technische Gründe, sich für die Freiheit zu entscheiden. Dies darf allerdings nicht missverstanden werden als Aufforderung zur Verbreitung rechtswidriger Inhalte im Internet. Toleranz wäre hier eine Schwäche.

Kopierschutztechniken, technische Nutzungsbeschränkungen und reaktive Verfahren zur Verfolgung (Internet-Kontrollen) sind momentan noch technisch mangelhaft und werden es solange sein, bis international anwend- und durchsetzbare Regeln gelten. Anbieter rechtswidriger Inhalte weichen bei Sperrung beispielsweise auf Server im Ausland aus. Das Internet ist faktisch ein internationales Netz. Wenn Schutzsysteme wirkungsvoll sein sollen, bedarf es erstens eines internationalen Konsens, was rechtswidrige Inhalte sind, und zweitens einer international anerkannten Organisation, die dafür sorgt, dass die Regeln international eingehalten werden.

Der Europarat hat auf die neuen Risiken beispielsweise mit der „Cybercrime Convention“ [11] reagiert, die der Anfang eines internationalen Regelungswerkes zur Verfolgung von Straftaten im und durch das Internet sein soll. Neben Verletzungen des Urheberrechts und der Bereitstellung anderer illegaler Inhalte soll vor allem auch die Verfolgung von Denial-of-Service-Angriffen verbessert werden. Dann wären auch Besitz und Herstellung von Anleitungen und Software zur Begehung von Computerkriminalität strafbar.

Ein weiterer Versuch zur Harmonisierung der Gesetze, die das Internet besser regulierbar machen sollen, ist die „Hague Convention on Jurisdiction and Foreign Judgements in Civil Matters“ [41]. Forderungen nach stärkeren Möglichkeiten, Internet-Benutzer zu kontrollieren, sind Ausdruck des Ohnmachtsgefühls der Regulierer, aber kein Mittel zur Stärkung des mündigen „Internet-Bürgers“.

Technisch mangelhafte Schutzsysteme werden dazu führen, dass Laien in die Sperre laufen. Technisch Versierte lassen sich durch verbesserte Kontrollmöglichkeiten nicht abschrecken. Etwas platt formuliert: Schwache Schutzsysteme schützen vor den Dummen und machen aus den vermeintlich Cleveren Helden.

Politische und gesellschaftliche Diskussion

Die politische und gesellschaftliche Diskussion zu den Folgen des Digital Rights Management wird national wie international auch heftig im Internet geführt. Eine Sammlung solcher Beiträge findet sich unter http://www.inf.tu-dresden.de/~hf2/drm/.

Eine der Botschaften lautet: Nichts ist fataler als ein falsches Sicherheitsgefühl bei den Menschen. Politische Entscheidungen für eine stärkere Kontrolle der Internet-Benutzer werden vielleicht das Sicherheitsgefühl der Menschen stärken, faktisch aber keine höhere technische Sicherheit bieten können.

Dank

Ein herzliches Dankeschön für kleinere und größere Zuarbeiten sowie Unterstützung bei der Recherche, Aufbereitung und Durchsicht des Manuskripts geht an Miriam Busch, Dr. Christian Dressel, Kristian Köhntopp und Stefan Köpsell.

Literaturverzeichnis

[1] D. G. Abraham, et al.: Transaction Security System. IBM Systems Journal 30/2 (1991) 206–229.

[2] Ross J. Anderson, Markus G. Kuhn: Tamper Resistance – a Cautionary Note. In: Proc. Second USENIX Workshop on Electronic Commerce. Oakland, California, Nov. 18–21 1996, 1–11.

[3] Urheberrecht in der Informationsgesellschaft. Gemeinsames Positionspapier von BDB und DBI, Juli 1998. http://www.dbi-berlin.de/dbi_ber/recht/urh-einl.htm.

[4] Stefan Bechthold: Vom Urheber- zum Informationsrecht – Implikationen des Digital Rights Management, Schriftenreihe Information und Recht 33. Verlag C. H. Beck, München, 2002.

[5] F. Beck: Integrated Circuit Failure Analysis – A Guide to Preparation Techniques. John Wiley & Sons, New York, 1998.

[6] S. Blythe, et al.: Layout Reconstruction of Complex Silicon Chips. IEEE Journal of Solid-State Circuits 28/2 (1993) 138–145.

[7] D. Boneh, M. Franklin: An efficient public key traitor tracing scheme. In: Advances in Cryptology – CRYPTO ’99, Lecture Notes in Computer Science 1666. Springer-Verlag, Berlin, 1999, 338–353.

[8] D. Boneh, J. Shaw: Collusion secure fingerprinting for digital data. IEEE Transactions on Information Theory 44/5 (1998) 1897–1905.

[9] Chipseal Tamper Resistant Composite, Dow Corning. http://www.se-com.com/secom/sp/dow.html.

[10] B. Chor, A. Fiat, M. Naor: Tracing traitors. In: Advances in Cryptology – CRYPTO ’94, Lecture Notes in Computer Science 839. Springer-Verlag, Berlin, 1994, 480–491.

[11] Draft Convention on Cybercrime. http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

[12] Ingemar Cox, Joe Kilian, Tom Leighton, Talal Shamoon: A Secure, Robust Watermark for Multimedia. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 185–206.

[13] Ingemar J. Cox, Jean-Paul M. G. Linnartz: Some General Methods for Tampering with Watermarks. IEEE Journal on Selected Areas in Communications 16/4 (1998) 587–593.

[14] J. H. Daniel, D. F. Moore, J. F. Walker: Focused Ion Beams for Microfabrication. Engineering Science and Education Journal (1998) 53–56.

[15] Lutz Donnerhacke, Steffen Peter: Vorsicht, Falle! iX 3 (1997) 90.

[16] Digital Video Broadcasting (DVB): Multimedia Home Platform (MHP) Specification 1.0. European Telecommunications Standards Institute, ETSI TS 101 812 V1.1.1 (2000-07).

[17] Cynthia Dwork, Jeffrey Lotspiech, Moni Naor: Digital Signets: Self-Enforcing Protection of Digital Information. In: Proc. 28th ACM Symposium on the Theory of Computing. Philadelphia, Pennsylvania, USA, 22.–24. Mai 1996, 489–498.

[18] Joachim Euchner: Proposal for an open MHP-Implementation. http://www.linuxtv.org/developer/mhp302.html.

[19] Hannes Federrath: Steganographie in Rechnernetzen. In: Tutorium „Sicherheit in Netzen“ der 13. DFN-Arbeitstagung über Kommunikationsnetze. Düsseldorf, 26.–28. Mai 1999. http://www.inf.tu-dresden.de/~hf2/publ/1999/Fede1_99DFNStego.pdf.

[20] Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. In: Günter Müller, Andreas Pfitzmann (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison-Wesley-Longman, 1997, 83–104. http://www.inf.tu-dresden.de/~hf2/publ/1997/FePf_97Baust/.

[21] Frank W. Felzmann: Die Task Force „Sicheres Internet“. KES Zeitschrift für Kommunikations- und EDV-Sicherheit 16/3 (2000) 61–68.

[22] H. P. Feuerbaum: Electron Beam Testing: Methods and Applications. Scanning 5/1 (1982) 14–24.

[23] Security Requirements for Cryptographic Modules. FIPS PUB 140-1, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U.S. Department of Commerce, 11. Jan. 1994.

[24] FITUG: IFPI Rights Protection System – A Compiled Fact Sheet. ftp://ftp.fitug.de/pub/eu/RPS02.PDF.

[25] E. Gafni, J. Staddon, Y. L. Yin: Methods for Integrating Traceability and Broadcast Encryption. In: Advances in Cryptology – CRYPTO ’99, Lecture Notes in Computer Science 1666. Springer-Verlag, Berlin, 1999, 372–387.

[26] Clemens Gleich: Entfesselte Musik – Microsofts neues Digital Rights Management ausgehebelt. ct 23 (2001) 62.

[27] Gore D^3 Electronic Security Enclosures. http://www.goreelectronics.com/products/specialty/electronic_security_enclosures.cfm.

[28] Peter Gutmann: Data Remanence in Semiconductor Devices. In: Proc. 10th Usenix Security Symposium. Washington, D.C., 13.–17. Aug. 2001.

[29] Heise-News: Schily empfiehlt Sofortmaßnahmen für sichereres Internet, 25. Apr. 2000. http://www.heise.de/newsticker/data/fm-25.04.00-000/.

[30] Identification cards – Integrated circuit(s) cards with contacts. ISO 7816, International Organization for Standardization, Geneva.

[31] D. Kahn: The Codebreakers – The Story of Secret Writing. Macmillan, New York, 1967.

[32] Auguste Kerckhoffs: La cryptographie militaire. Journal des sciences militaires, Vol. IX, 5–38, Jan. 1883, 161–191, Feb. 1883. http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/.

[33] Will Knight: Sony locks CDs to stop internet copying. The New Scientist Online. http://www.newscientist.com/news/news.jsp?id=ns99991336.

[34] P. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Advances in Cryptology – CRYPTO '96, Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1996, 104–113.

[35] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis. In: Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science 1666. Springer-Verlag, Berlin, 1999, 388–397.

[36] Kristian Köhntopp, Marit Köhntopp, Martin Seeger: Sperrungen im Internet. Datenschutz und Datensicherheit DuD 21/11 (1997) 626–631.

[37] Oliver Kömmerling, Markus G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. In: Proc. USENIX Workshop on Smartcard Technology (Smartcard '99). USENIX Association, Chicago, Illinois, USA, 10.–11. Mai 1999, 9–20.

[38] D. Kosiur: IP Multicasting. Wiley, 1998.

[39] Markus Kuhn, Fabian Petitcolas: Stirmark, 1997. http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/.

[40] Petra Labriga: Die Britische Nationalbibliothek auf dem Weg zur elektronischen Bibliothek. Bibliotheksdienst /6 .

[41] Julia Lawlor: From the Trenches: Do laws know no bounds?, 16. Okt. 2001. http://www.redherring.com/index.asp?layout=story_imu&doc_id=1570020357&channel=10000001.

[42] Macrovision Video Copy Protection. http://www.macrovision.com/solutions/video/copyprotect/.

[43] D. P. Maher: Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective. In: Proc. Financial Cryptography, FC '97, Lecture Notes in Computer Science 1318. Springer-Verlag, Berlin, 1997, 109–121.

[44] Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist. Datenschutz und Datensicherheit DuD 18/6 (1994) 318–326.

[45] Moni Naor, Benny Pinkas: Threshold Traitor Tracing. In: Proc. 18th Annual International Cryptology Conference, Lecture Notes in Computer Science 1462. Springer-Verlag, Berlin, 1996, 502–517.

[46] Antti Paarlahti: Macrovision FAQ, v1.1, Tampere, Finland, 1995. http://ee.tut.fi/~pam/macrovision/macrov_faq_v1.1.txt.

[47] Fabien A. P. Petitcolas, Ross Anderson, Markus G. Kuhn: Attacks on copyright marking systems. In: David Aucsmith (Hg.): Proc. 2nd Workshop on Information Hiding, Lecture Notes in Computer Science 1525. Springer-Verlag, Berlin, 1998, 218–238.

[48] Birgit Pfitzmann: Trials of traced traitors. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 49–64.

[49] Birgit Pfitzmann, Michael Waidner: Kopierschutz durch asymmetrische Schlüsselkennzeichnung mit Signeten. In: Verläßliche IT-Systeme, GI-Fachtagung VIS ’97, DuD Fachbeiträge. Vieweg-Verlag, Wiesbaden, 1997, 17–32.

[50] Birgit Pfitzmann, Michael Waidner: Kopierschutz durch asymmetrisches Fingerprinting. Datenschutz und Datensicherheit DuD 22/5 (1998) 258–264.

[51] H. Reinitzer: Papierzerfall – Kulturzerfall? Über die Probleme der Bewahrung des ‚geistigen Erbes‘. Bibliotheksdienst 28/12 (1994) 1911–1925.

[52] Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2. Aufl. John Wiley & Sons, New York, 1996. (Die deutsche Übersetzung ist bei Addison-Wesley-Longman erschienen.).

[53] Sergei Skorobogatov: Low Temperature Data Remanence in Static RAM. University of Cambridge Computer Laboratory, 2001. http://www.cl.cam.ac.uk/~sps32/sram_article.pdf.

[54] Joshua Smith, Barrett Comiskey: Modulation and Information Hiding in Images. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, LNCS 1174. Springer-Verlag, Berlin, 1996, 207–226.

[55] Viktor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols. ACM Computing Surveys 15/2 (1983) 135–170.

[56] Steve H. Weingart: Physical Security for the μABYSS System. In: Proc. 1987 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 27.–29. Apr. 1987, 52–58.

[57] Jian Zhao: Look, it’s not there. Byte 22/1 (1997) 7–12.