Die Technik von Zugangskontrolldiensten

Hannes Federrath

Freie Universität Berlin · Institut für Informatik

Erscheint als: „Erster Teil. Technische Grundlagen“ in: Dressel, Scheffler (Hrsg.): *Rechtsschutz gegen Dienstepiraterie – Das ZKDSG in Recht und Praxis*. Verlag C. H. Beck, München, 2003.

Inhaltsverzeichnis

Erster Teil. Technische Grundlagen

1 Einführung

Durch Zugangskontrolle kann der Zugang zu einem informationstechnischen System (IT-System) von einer vorherigen Erlaubnis abhängig gemacht werden. Mit dem Zugangskontrolldiensteschutzgesetz (ZKDSG) werden Zugangskontrolldienste und zugangskontrollierte Dienste (die Dienste, die nach erfolgreicher Zugangskontrolle genutzt werden) rechtlich besonders geschützt. Zugangskontrolldienste sollen in diesem Zusammenhang die unbefugte Inanspruchnahme und das Erschleichen der Nutzung von Rundfunkangeboten sowie Telediensten verhindern.

Um das Weitergeben und Vervielfältigen einer Nutzungsberechtigung nicht unnötig leicht zu machen, werden die bei der Zugangskontrolle zu überprüfenden Kennungen meist auf einem kleinen Gerät (z.B. Chipkarte, auch Smartcard genannt) hinterlegt, das physisch gesichert sein muss.

Damit die Inhalte bei der Übertragung zum berechtigten Nutzer nicht unberechtigt mitgelesen werden können, müssen sie verschlüsselt übertragen werden. Nach der erfolgreichen Berechtigungsprüfung ist der Benutzer in der Lage, die empfangenen Inhalte zu entschlüsseln.

Im folgenden werden nach einer Einführung die technischen Grundlagen von Zugangskontrolldiensten erläutert (Abschnitt 2), ihre Anwendungsmöglichkeiten (Abschnitt 3) und einige Angriffe (4) auf sie beschrieben. In Abschnitt 5 wird eine kurze Bewertung des ZKDSG aus technischer Sicht vorgenommen und in Abschnitt 6 die wesentlichen Aussagen noch einmal abschließend zusammengefasst.

1.1 Übertragungsmodell

Bevor die Inhalte konsumiert werden können, müssen sie zum Nutzer gelangen. Die Verteilung von Inhalten kann grundsätzlich Offline (mittels Datenträger) und Online (mittels Rundfunk- oder Satellitenübertragung, über spezielle Verteilkabel, Telefon oder das Internet) erfolgen. Im Bereich der Teledienste und Rundfunkangebote ist nur die Online-Verteilung interessant. Online verteilte Inhalte können synchron und asynchron konsumiert werden. Diese Unterscheidung bezieht sich auf den zeitlichen Zusammenhang zwischen Datenübertragung und Konsumierung:

- **Asynchron:** Inhalte, die auf einem Webserver zum Abruf gespeichert sind, können jederzeit angefordert und 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 noch nach Simulcasting und Webcasting. Unter Simulcasting wird die zeitgleiche Übertragung von terrestrischen Sen-

dungen im Internet verstanden, während mit Webcasting die Nur-Internet-Übertragung gemeint ist.

Weiterhin ist zu unterscheiden, ob alle Konsumenten exakt gleiche Kopien des Inhalts erhalten oder ob sie individualisierte, d.h. speziell auf sie zugeschnittene Kopien (z.B. mit eingebetteten Informationen über Kaufdatum, Besitzer etc.) erhalten. Bei der Verteilung von Rundfunkangeboten und beim Simulcasting erhalten alle Kunden aus Mangel an Übertragungsbandbreite den exakt gleichen Inhalt.

In Abbildung 1 ist der typische Ablauf der Erzeugung, Bereitstellung, Übertragung und Nutzung von Inhalten dargestellt.

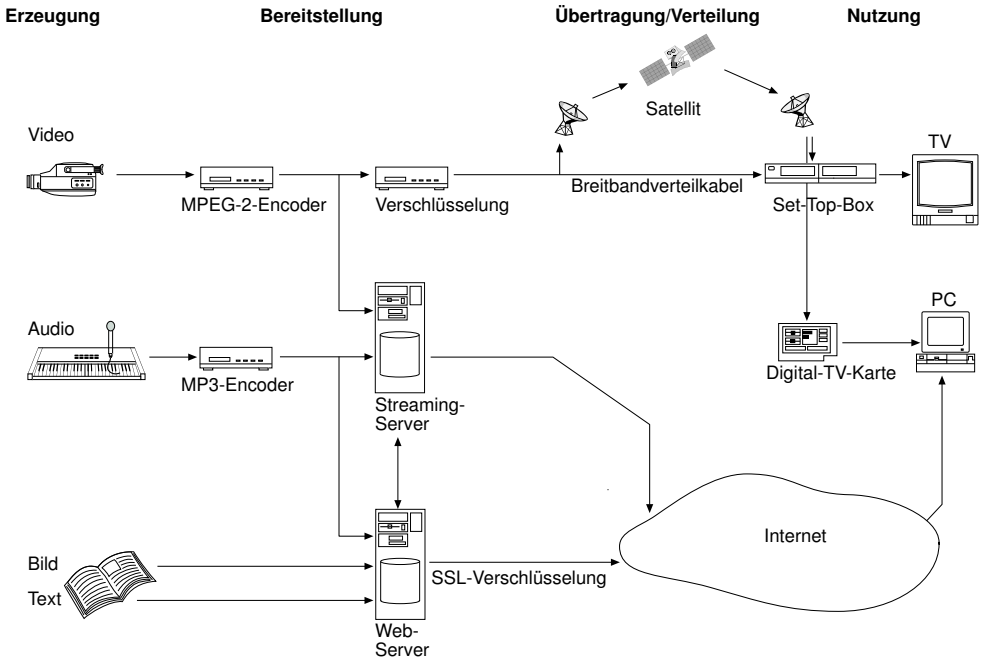

Abbildung 1: Erzeugung, Bereitstellung, Übertragung und Nutzung von Inhalten

Die Zugangskontrolle hat bei der Verteilung und Nutzung der Inhalte (unterschieden nach Rundfunkangeboten und Telediensten) folgende Aufgaben:

- Bei **verschlüsselten Rundfunkangeboten** wird der Inhalt senderseitig mit einem Medienschlüssel, der regelmäßig gewechselt wird, verschlüsselt. Jeder berechtigte Nutzer erhält vom Inhalteanbieter ein ausforschungssicheres Gerät (Smartcard, Set-Top-Box) zur Zugangskontrolle, das über eine eindeutige Seriennummer und Schlüssel verfügt. Die Zugangskontrolle besteht dann im Wesentlichen entweder darin, den berechtigten Nutzern den aktuellen Medienschlüssel mitzuteilen, oder dem Entschlüsselungsalgorithmus im der Smartcard oder der Set-Top-Box über das Ausstrahlen der berechtigten Seriennummern mitzuteilen, dass der Kunde empfangsberechtigt ist. Die Verschlüsselung findet meistens

mit proprietären und geheimgehaltenen Verschlüsselungsverfahren (z.B. Irdeto oder Betacrypt) statt.

- Bei **zugangskontrollierten Telediensten** wird entweder lediglich ein Passwort überprüft, das der Benutzer z.B. in einem Web-Browser eingeben muss, oder das Prüfen der Nutzungsberechtigung wird ebenfalls mittels Smartcard vorgenommen. Letzteres findet man im Internet derzeit noch recht selten (beispielsweise beim Home Banking Computer Interface, HBCI). Weit verbreitet sind Chipkarten-basierte Zugangskontrollsysteme beispielsweise in GSM-Mobilfunknetzen (Global System for Mobile Communication). Zur Authentikation wird im GSM z.B. der Algorithmus A3 angewendet. Beim HBCI kommen digitale Signatursysteme zum Einsatz. Die Verschlüsselung der Inhalte findet im Bereich Internet meistens mittels SSL (Secure Sockets Layer) statt, in anderen Kommunikationsnetzen auf Basis proprietärer Verschlüsselungsverfahren (im GSM beispielsweise mit dem Algorithmus A5).

1.2 Zugangskontrolle und Identifikation

Unter Zugangskontrolle versteht man, dass ein IT-System die Identitäten seiner Kommunikationspartner erfragt, prüft und nur mit berechtigten Partnern weiter kommuniziert. Kommunikationspartner können Menschen oder individuell an einen Menschen ausgegebene IT-Systeme (Smartcards) zur Berechtigungsprüfung sein. Merkmale zur Identifikation von Menschen können biometrische Merkmale (Was man ist), Wissen (Was man weiß) oder Besitz (Was man hat) sein. Die Tabelle 1 gibt einen Überblick über die wichtigsten Identifikationsmerkmale.

Was man ist	**Was man hat**	**Was man weiß**
Handgeometrie	Papierdokument	Passwort
Fingerabdruck	Metallschlüssel	Antworten auf Fragen
Aussehen	Magnetstreifenkarte	Rechenergebnisse für Zahlen
Eigenhändige Unterschrift	Chipkarte	
Retina-Muster		
Stimme		
Tipp-Charakteristik (Tastenanschlag)		
DNA-Muster		

Tabelle 1: Systematisierung wichtiger Identifikationsmerkmale

Die in IT-Systemen derzeit noch am häufigsten vorkommende Form der Identifizierung ist das Passwort. Bei Abonnenten-TV-Angeboten und im GSM-Mobilfunk erhält der Kunde eine Smartcard mit einer individuellen Identifikationsnummer und darauf enthaltenen kryptographischen Schlüsseln.

Um Menschen die Möglichkeit zu geben, IT-Systeme zu identifizieren, kommen die in Tabelle 2 genannten Möglichkeiten in Betracht.

Was es ist	Was es weiß	Wo es steht
Gehäuse	Passwort	Standort
Siegel	Antworten auf Fragen	
Hologramm	Rechenergebnisse für Zahlen	
Verschmutzung		

Tabelle 2: Identifikation von IT-Systemen durch Menschen

Auch IT-Systeme sollen sich gegenseitig identifizieren können. Die wichtigste der in Tabelle 3 genannten Möglichkeiten ist die Kryptographie, auf die später auch näher eingegangen wird. Dabei wird meist das Vorhandensein eines Geheimnisses beim Kommunikationspartner überprüft, ohne dies übertragen zu müssen (Challenge-Response-Authentikation, siehe Abschnitt 3.3). Auf diese Weise wird beispielsweise die Echtheit der an einen Nutzer ausgegebenen Smartcard überprüft.

Was es weiß	Leitung woher
Passwort	Verbindung mit anderen Geräten
Antworten auf Fragen	
Rechenergebnisse für Zahlen	
Kryptographie	

Tabelle 3: Identifikation von IT-Systemen durch IT-Systeme

1.3 Interessen der Beteiligten

Bei der technischen Ausgestaltung von Zugangskontrolldiensten sind im Wesentlichen die Schutzinteressen des Inhalte-Anbieters und der Nutzer zu berücksichtigen:

1. Interessen des **Inhalte-Anbieters**:
   - Verhindern unberechtigter Nutzung des Dienstangebots,
   - Rückruf einer Nutzungsberechtigung bzw. Vergabe auf Zeit,
   - Verfolgbarkeit einer Sicherheitsverletzung,
   - Updaten der Hardware/Software im Fall einer erkannten Sicherheitsschwäche,
2. Wahrung der Schutzinteressen des **Nutzers**:
   - keine unberechtigte Verdächtigung/Verantwortung für nicht begangene Sicherheitsverletzungen,
   - Datenschutz, d.h. die Bildung von Nutzungs- und Interessensprofilen sollte vermieden werden,
   - Investitionsschutz, d.h. die Geräte, die der Nutzer erworben hat, müssen ihm über einen angemessenen Zeitraum den Konsum der Inhalte ermöglichen.

1.4 Abgrenzung zu anderen Mechanismen

Zugangskontrolldienste dienen nicht dem Schutz von Inhalten vor unberechtigtem Mitlesen (Vertraulichkeit) oder vor Verfälschung (Integrität). Hierzu werden Verschlüsselungsverfahren (Abschnitt 2.2) und Message Authentication Codes (MACs, Abschnitt 2.3) eingesetzt.

Zugangskontrolldienste sind keine Kopierschutzsysteme, d.h. alle Daten, die über Kommunikationsnetze, Verteilnetze, Radiowellen oder Datenträger übertragen werden, können beliebig (auch von Unberechtigten) kopiert werden. Daraus ergibt sich die Anforderung, dass die Nutzdaten verschlüsselt sein müssen und erst nach Freigabe durch den Zugangskontrolldienst vom berechtigten Empfänger entschlüsselt werden können.

Verschlüsselungsverfahren (oder genereller kryptographische Verfahren) sind auch Bestandteile eines sicheren Zugangskontrolldienstes, bei dem einem Angreifer das Erschleichen der Nutzung von Rundfunkangeboten, Informations- und Kommunikationsdiensten möglichst schwer gemacht werden soll: Ein starker Zugangskontrolldienst, der nach dem aktuellen Stand der Technik arbeitet, wird sehr wahrscheinlich ebenfalls unter Verwendung kryptographischer Verfahren realisiert sein.

2 Beschreibung der technischen Komponenten

Im folgenden werden die wichtigsten technischen Komponenten von Zugangskontrolldiensten beschrieben: Ausforschungssichere Hardware, Verschlüsselungsverfahren und Message Authentication Codes.

2.1 Ausforschungssichere Hardware

Der Besitz einer Smartcard (eigentlich: der Besitz des auf der Karte enthaltenen geheimen Schlüssels oder der für den Kunden unveränderlichen Identifikationsnummer) ermöglicht dem Kunden den Zugang zum kostenpflichtigen TV-Angebot. Um zu verhindern, dass ein böswilliger Kunde den Schlüssel aus der Smartcard ausliest und ihn illegal weiterverbreitet, muss die Karte (bzw. der Schlüssel) ausforschungssicher gebaut sein (**Tamper Resistance**). Dies erfordert physische Sicherungsmaßnahmen.

Angriffe auf die physische Sicherheit werden durch Schirmung (z.B. gegen elektromagnetische Abstrahlung), Erkennen und Bewerten (z.B. durch entsprechende Sensoren) sowie Verzögern des Angriffs (z.B. durch hartes Material) erschwert. Bei erfolgreichen Angriffen können als letzte Maßnahme die gespeicherten Geheimnisse gelöscht werden (Abbildung 2).

Die Schirmung gegen elektromagnetische Abstrahlung wird beispielsweise durch Aufdampfen von Metallschichten auf den Chip erreicht. Das Verzögern des Angriffs erreicht man durch Eingießen in eine Schutzhülle aus Plastik oder Harz. Selbst wenn das Freilegen des Innern eines Chips gelingt, kann ein spezielles, mehrschichtiges Chipdesign den Zugriff mittels sog.

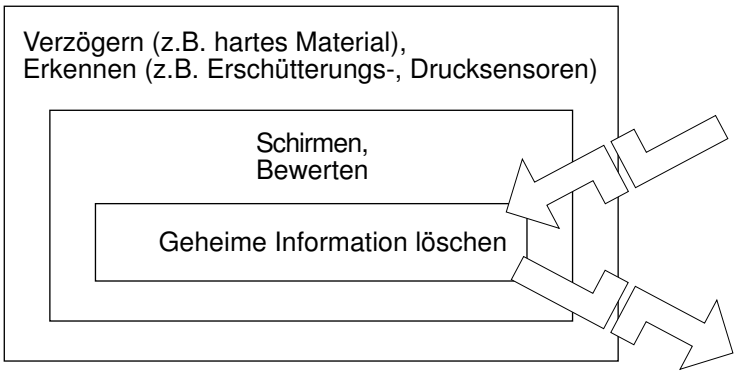

Abbildung 2: Schichtenstruktur physischer Sicherungsmaßnahmen

Mikroprobing-Nadeln auf die Busleitungen oder Speicherzellen (in der die Schlüssel abgelegt sind) verhindern oder wenigstens erschweren: Oberhalb und unterhalb der Schicht, in der die geheimen Daten liegen, wird ein Geflecht aus Leiterbahnen aufgebracht, so dass der Chip bei einer Zerstörung (Kurzschluss oder Unterbrechung) dieser Leiterbahnen die Arbeit verweigert.

Da dem Angreifer u.U. viel Zeit (im Bereich von Monaten oder gar Jahren) zum Angriff zur Verfügung steht und er außerdem in vielen Fällen beim Angriff die Zerstörung des Gerätes riskieren kann, ohne entdeckt zu werden, ist die Abwehr solcher Angriffe mit sehr hohem Aufwand verbunden und dauerhaft praktisch nicht möglich, da jederzeit neuartige Angriffsmöglichkeiten entdeckt werden können.

Bei Smartcards konnte z.B. durch Messung des Stromverbrauchs der Karte während eines Verschlüsselungsvorgangs der ebenfalls nur auf der Karte vorhandene Schlüssel ermittelt werden, obwohl dies die Smartcard eigentlich hätte verhindern sollen (**Power Analysis**, [8]). Da (vereinfacht gesagt) je nach Belegung (0 oder 1) des aktuell vom Verschlüsselungsalgorithmus verwendeten Schlüsselbits die Stromaufnahme der Karte schwankte, konnten die Schlüsselbits mit einem schnell reagierenden Amperemeter direkt abgelesen werden.

Eine nicht auf Smartcards beschränkte, aber dort aufgrund der geringeren Komplexität ggf. leichter als bei PCs mögliche Angriffsklasse sind die **Timing Attacks**. So können beispielsweise Verzweigungen des Programmcodes innerhalb des Ver- oder Entschlüsselungsalgorithmus beim Angreifer zu einem Informationsgewinn über den Schlüssel führen [7].

Eine sehr problematische Angriffsklasse sind die **Fault Induction Attacks** [10]. In Labors wurde gezeigt, dass die physische Sicherheit geheimer Daten auf Smartcard in der Praxis nicht die erwartete und erwünschte Stärke besitzt [1]. So gelingt es beispielsweise mit Hilfe chemischer Substanzen oder Ionenstrahlung, Schutzschichten, die das Auslesen der geheimen Informationen direkt vom Chip verhindern sollen, zu entfernen bzw. zu umgehen. Hierzu werden zunächst die Kontaktflächen der Smartcard freigelegt, die Kontakte herausgeführt und an ein Emulatorsystem angeschlossen. Mit Hilfe von Mikroprobing-Metallnadeln unter einem Mikroskop oder mittels eines Elektronenstrahltesters werden die Busleitungen des Prozessors angezapft und es kann der

geheime Speicherinhalt mitprotokolliert werden.

In [13] konnte sogar gezeigt werden, dass für solche Angriffe keine teure Ausstattung notwendig ist. Mit Hilfe des in einer Kleinbildkamera eingebauten Blitzlichtes gelang es, das Innere eines freigelegten Chips derart mit Lichtblitzen zu beschießen, dass dadurch gezielte Manipulationen möglich wurden. Mit Hilfe eines Mikroskops konnte der Blitz so fokussiert werden, dass das Bit einer Speicherzelle von 1 auf 0 gesetzt werden konnte. War das Bit bereits 0, trat durch den Blitz keine Veränderung auf. Handelt es sich hierbei um die Bits eines zu knackenden Schlüssels, hat das fatale Folgen für dessen Geheimhaltung, da es jetzt möglich ist, sukzessive die Belegung jedes einzelnen Bits zu ermitteln: Nacheinander werden alle Bits durch den Lichtblitz auf 0 gesetzt und immer wieder eine zuvor gewählte Nachricht verschlüsselt. Wenn sich durch den Lichtblitz der Schlüsseltext ändert, war das Bit 1, sonst 0. Ein solcher Angriff gelingt, weil sich der Wert eines Bits (0 oder 1) durch die Spannung (niedrig/low/L oder hoch/hight/H) auf einer „Leitung“ ergibt. Um solche Angriffe zu verhindern, schlagen [13] vor, für jedes Bit ein Paar vorzusehen, wobei die Kombinationen (HL) und (LH) jeweils einem logischen Wert zugeordnet sind und die Kombination (HH), die bei einem Lichtblitz entstehen würde, einem Alarmzustand entspricht, in dem der Chip zurückgesetzt wird oder die Arbeit verweigert.

2.2 Verschlüsselung

Ziel der Verschlüsselung ist es, Daten so vom Sender zum Empfänger zu übermitteln, dass niemand auf der Übertragungsstrecke deren Inhalt mitlesen kann. Die Verschlüsselung von Daten erfolgt mittels kryptographischer Verfahren. Der Absender und Empfänger eines Inhalts einigen sich auf einen bestimmten Verschlüsselungsalgorithmus, der öffentlich und damit auch dem potentiellen Angreifer bekannt sein darf. Die Geheimhaltung der Nachricht hängt einzig und allein von der Geheimhaltung eines Parameters, dem Schlüssel, ab. Dieser wichtige Grundsatz (Geheimhaltung des Schlüssels, Offenlegung des Algorithmus, genannt Kerckhoffs-Prinzip) geht zurück auf Auguste Kerckhoffs [6]. Ziel dabei ist es, einen möglichst ausgereiften Algorithmus zu verwenden. Um nicht von verborgenen Schwächen überrascht zu werden, sollte der Algorithmus einer breiten Fachöffentlichkeit zur Begutachtung und ggf. Verbesserung vorliegen. Dass dies durchaus sinnvoll ist, beweisen beispielsweise die Schwächen des im GSM-Mobilfunk angewendeten Verschlüsselungsalgorithmus A5, der inzwischen auf einem durchschnittlich leistungsfähigen PC mit 160 Gigabyte Festplattenspeicher in Echtzeit geknackt werden kann [3].

Man unterscheidet symmetrische und asymmetrische Verschlüsselungsalgorithmen. Bei symmetrischen Verschlüsselungsalgorithmen besitzen Sender und Empfänger einen identischen geheimen Schlüssel (Abbildung 3). Dieser Schlüssel wird in einem Algorithmus zur Schlüsselgenerierung erzeugt, der durch eine Zufallszahl parametrisiert ist.

Bei asymmetrischen Verschlüsselungsalgorithmen erzeugt sich der spätere Empfänger entsprechend einer vom Verschlüsselungsalgorithmus abhängigen Rechenvorschrift ein Schlüsselpaar. Der eine Teil dient zur Verschlüsselung und wird veröffentlicht (öffentlicher Verschlüsselungsschlüssel). Der andere Teil dient zur Entschlüsselung und wird vom Empfänger geheimgehal-

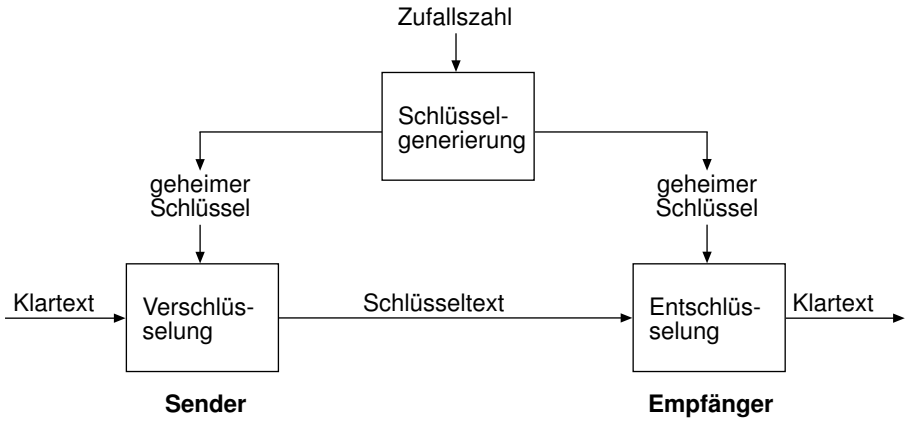

Abbildung 3: Symmetrische Verschlüsselung

ten (privater Entschlüsselungsschlüssel). Nun kann jeder, der den öffentlichen Verschlüsselungsschlüssel kennt, an den Empfänger eine verschlüsselte Nachricht schicken, die der Empfänger (und nur er) mit dem privaten Entschlüsselungsschlüssel entschlüsseln kann (Abbildung 4).

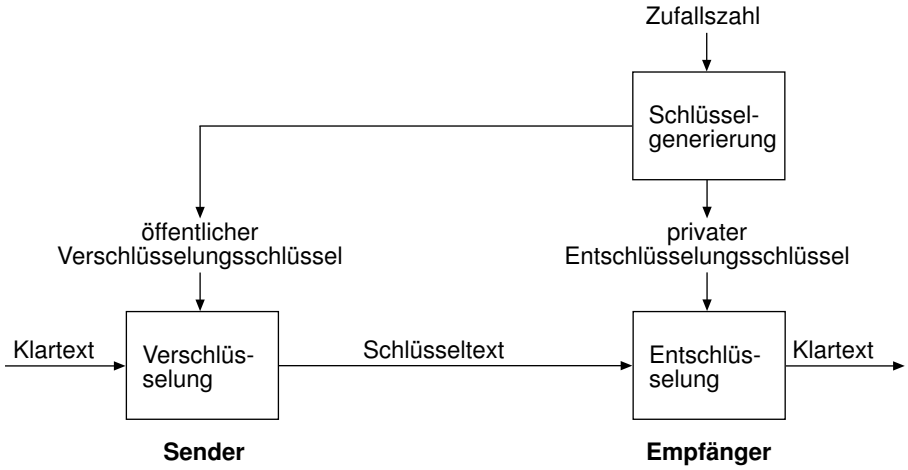

Abbildung 4: Asymmetrische Verschlüsselung

Beispiele für symmetrische Verfahren sind DES, IDEA, Triple-DES und AES. Das bekannteste asymmetrische Verfahren ist RSA. Beispielsweise in [12] werden die Algorithmen der wichtigsten Verfahren genau erklärt. Die asymmetrische Verschlüsselung ist deutlich rechenaufwendiger als die symmetrische. Dagegen vereinfacht die asymmetrische Verschlüsselung den Schlüsselaustausch erheblich, da keine geheimen Schlüssel ausgetauscht werden müssen. Die derzeit als sicher geltenden Schlüssellängen bei symmetrischen Verfahren bewegen sich im Bereich 112–256 Bit, bei asymmetrischen Verfahren zwischen 1024 und 2048 Bit.

Im Bereich des Abonnenten-TV werden heute aus Effizienzgründen symmetrische Verfahren

eingesetzt. Auf einer Smartcard ist der Entschlüsselungsalgorithmus vorhanden und der geheime Schlüssel gespeichert. Zum Entschlüsseln wird die verschlüsselte Nachricht in die Karte geladen, dort entschlüsselt und ausgegeben. Bei der verschlüsselten Nachricht handelt es sich meist wiederum um einen Schlüssel, den sog. Sitzungs- oder Medienschlüssel (siehe auch Abschnitt 3.2). Im regulären Betrieb verlässt der geheime Schlüssel bei einem sicheren System also niemals die Smartcard und kann auch niemals direkt ausgelesen werden. Die physische Geheimhaltung des Schlüssels ist essentiell für die Verhinderung des unberechtigten Zugangs zu den kostenpflichtigen Inhalten.

Trotz des Kerckhoffs-Prinzips hat sich die Geheimhaltung der eingesetzten Algorithmen bei einigen Smartcard-basierten Pay-TV-Systemen in der Vergangenheit als Sicherheitsvorsprung bewährt. Weil 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. 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. Dies macht einen konkreten Angriffsversuch erheblich aufwendiger, weil zunächst die Funktionsweise des Algorithmus rekonstruiert werden muss (Reverse Engineering).

2.3 Authentikation

Durch Verschlüsselung kann der Inhalt einer Nachricht vertraulich übermittelt werden. Durch Authentikation kann die Echtheit (Unverfälschtheit) einer Nachricht geprüft werden. Somit ist niemand mehr unerkannt in der Lage, Nachrichten auf der Übertragungsstrecke zu verändern oder gar gefälschte Nachrichten zu senden. Der Sender fügt der Nachricht einen Prüfteil bei, der von einem vorher zwischen Sender und Empfänger ausgetauschten geheimen, symmetrischen Schlüssel abhängt (Abbildung 5).

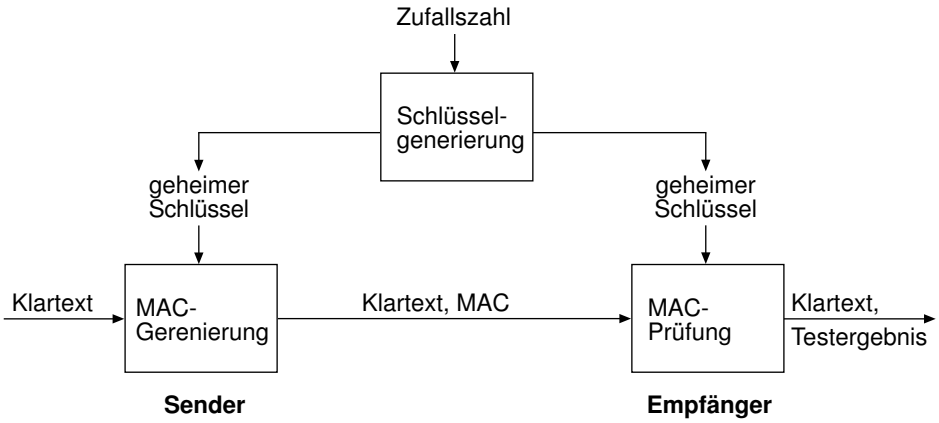

Abbildung 5: Message Authentication Codes (MACs)

Diese Prüfsumme wird Message Authentication Code (MAC) genannt. Ohne Kenntnis des Schlüssels kann der Angreifer zu einer von ihm gewählten Nachricht nicht den passenden MAC erzeugen. Somit wird die Nachricht beim Empfänger als gefälscht erkannt und weggeworfen.

Mit einem solchen Authentikationssystem ist es mittels eines interaktiven Protokolls (Challenge-Response-Authentikation, siehe auch Abschnitt 3.3) möglich, beim Kommunikationspartner den Besitz eines Geheimnisses (konkret des geheimen Schlüssels) zu überprüfen, ohne dieses selbst übertragen zu müssen. Nur der Besitzer des Geheimnisses kann die Zugangskontrolle passieren. Da das Geheimnis selbst jedoch nicht übertragen wird, kann die Kommunikation während der Authentikation unverschlüsselt erfolgen. Dies ist gegenüber passwortbasierten Verfahren ein Vorteil.

3 Typische Varianten von Zugangskontrolle

Im folgenden werden drei typische Grundverfahren von Zugangskontrolldiensten vorgestellt.

3.1 Passworte

Ein Mensch erhält bei der Buchung eines Dienstes ein Passwort. Um den Dienst zu nutzen, muss er das Passwort eingeben. Der Dienstanbieter prüft, ob das Passwort korrekt ist, und der Dienstnutzer erhält anschließend Zugang (Abbildung 6). Dieses Verfahren wird beispielsweise beim Computer-Login angewendet.

Die Daten werden meist unverschlüsselt übertragen. Da das Passwort leicht abgefangen werden kann, ist ein solcher Zugangskontrolldienst sehr unsicher, sobald auf der Übertragungsstrecke zwischen Dienstanbieter und Dienstnutzer mitgelesen werden kann. Es ist jedoch auch Verschlüsselung möglich: Sollen beispielsweise Dienstangebote im World Wide Web geschützt werden, kann mittels Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS), zu erkennen an einer URL, die mit https (anstelle von http) beginnt, die gesamte Kommunikation inkl. der Passwortabfrage verschlüsselt werden.

Ein solcher Zugangskontrolldienst eignet sich für die Absicherung von individuell angebotenen Informations- und Kommunikationsdiensten sowie für im Internet angebotene Rundfunkangebote. Voraussetzung ist, dass die Abspielsoftware über entsprechende Funktionen zur Entschlüsselung des Datenstroms verfügt. Rundfunkangebote, die über Breitbandverteilkabel, Satellit oder terrestrische Ausstrahlung verteilt werden, können mit diesem Verfahren nicht abgesichert werden, solange kein Kommunikationskanal („Rückkanal“) vom Nutzer zum Dienstanbieter vorhanden ist, über den die Passwortabfrage erfolgen könnte.

Die Verwendung von Passworten zur Zugangskontrolle ist sehr unsicher gegen Missbrauch, da ein Nutzer einfach sein Passwort weitergeben kann, um anderen Benutzern Zugang zu verschaffen. Zumindest bei Diensten, in denen die Nutzung pauschal berechnet wird oder keine weiteren

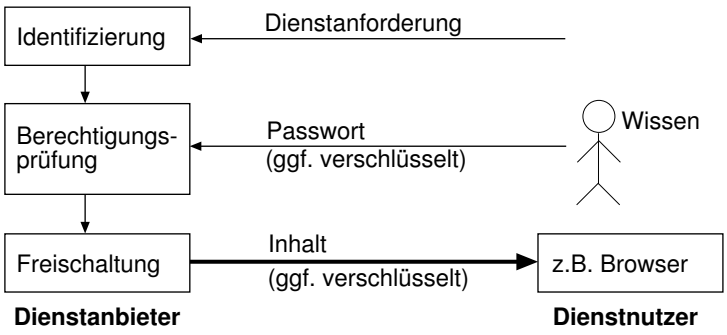

Abbildung 6: Zugangskontrolle mittels Passwort

Kosten verursacht, entsteht für den berechtigten Nutzer dadurch kein unmittelbarer finanzieller Schaden.

3.2 Smartcards mit Master-Key

Ein Mensch erhält bei der Buchung eines Dienstes ein (kleines) Gerät (z.B. eine Smartcard). In diesem Gerät sind eine Seriennummer sowie ein oder mehrere kryptographische Entschlüsselungsschlüssel gespeichert. Die Berechtigungsprüfung erfolgt auf der Seite des Nutzers, indem der empfangene Datenstrom mit einem der auf dem Gerät befindlichen Entschlüsselungsschlüssel erfolgreich entschlüsselt werden kann (Abbildung 7). Das bedeutet, alle empfangenen verschlüsselten Daten werden durch die Smartcard geleitet. Es wird somit keine explizite Berechtigungsprüfung vorgenommen, sondern eher eine implizite.

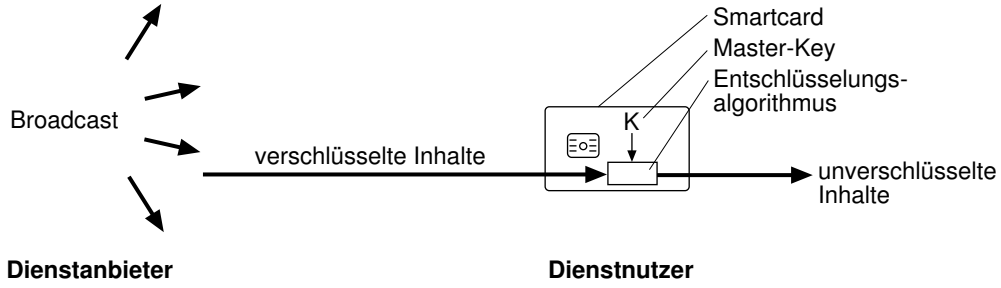

Abbildung 7: Zugangskontrolle mittels Smartcards mit Master-Key

Bei Bedarf kann die Smartcard noch durch die Eingabe einer persönlichen Identifikationsnummer (PIN) vor unberechtigter Nutzung gesichert werden.

Um eine geräteindividuelle Zugangskontrolle zu ermöglichen (beispielsweise, um einem Nutzer nur bestimmte Sendungen eines Programms, für die er bezahlt hat, zugänglich zu machen), können in den Datenstrom die Seriennummern aller berechtigten Geräte eingebettet werden. Vor

der Ausgabe des unverschlüsselten Datenstroms prüft die Smartcard, ob die eigene Seriennummer gesendet wurde und gewährt somit den Zugang. Das umgekehrte Vorgehen (Senden von Sperrlisten) ist ebenfalls möglich. Das schwächste Glied eines solchen Verfahrens ist der auf allen in Umlauf gegebenen Smartcards gleiche Master-Key. Sobald er kompromittiert ist, kann der Inhalt beispielsweise mit Hilfe nachgebauter oder entsprechend programmierter Smartcards (Abschnitt 4.2) auch ohne Berechtigung genutzt werden. Dabei wird die Abfrage nach gültigen Seriennummern einfach umgangen.

Die in der Praxis angewendeten Verfahren sind unwesentlich komplizierter als die geschilderte Grundidee. So soll eine Hierarchie aus Schlüsseln die Kompromittierung des Gesamtsystems bei Bekanntwerden einzelner Schlüssel (Gruppenschlüssel) erschweren (Abbildung 8). Der eigentliche Inhalt wird mit einem nur für kurze Zeit gültigen Sitzungsschlüssel (auch Medienschlüssel genannt) verschlüsselt. Der Medienschlüssel wird wiederum mit dem Master-Key verschlüsselt und als Metadaten (im Abonnenten-TV Electronic Control Message, ECM, genannt) vor der Übertragung der Inhalte übermittelt. Der Dienstnutzer entschlüsselt den Medienschlüssel auf seiner Smartcard und hat so Zugriff auf den Inhalt. Der Inhalt selbst kann im Empfänger (Set-Top-Box) bzw. im Conditional-Access-Modul (CAM, einer genormten, aber anbieterabhängigen Einschubkarte für programmanbieter-unabhängige Set-Top-Boxen) entschlüsselt werden. Somit müssen nicht alle Inhaltsdaten über die Smartcard entschlüsselt werden, deren Prozessor bzw. Kommunikationsschnittstelle dafür auch nicht leistungsfähig genug wäre.

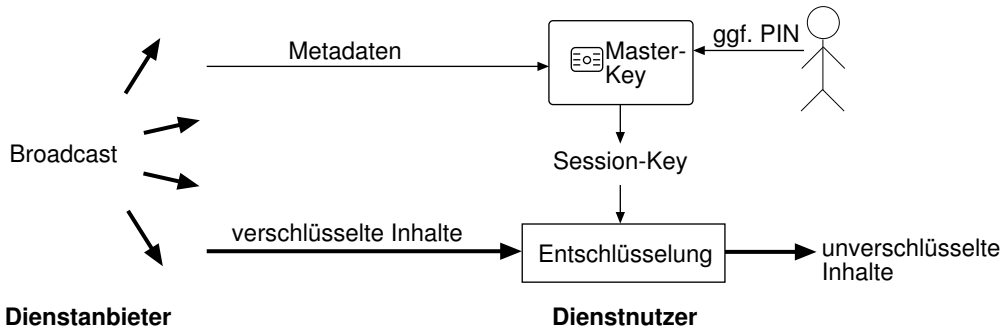

Abbildung 8: Zugangskontrolle mittels Smartcards mit Master-Key und Session-Key

Es existieren mehrere Master-Keys für Gruppen von Nutzern. Somit ist es (theoretisch) bei kompromittiertem Master-Key möglich, ab sofort für diesen Master-Key keine verschlüsselten Medienschlüssel mehr zu broadcasten. Somit wird diese Nutzergruppe ausgeschlossen. Praktisch müssten aber die Smartcards der ehrlichen Benutzer der Gruppe vorher ausgetauscht werden, damit diese nicht plötzlich vom Empfang ausgeschlossen sind.

Um Missbrauch zu verhindern, muss die Smartcard physisch so aufgebaut sein, dass der Nutzer keine Möglichkeit hat, die innere Struktur und insbesondere die darin gespeicherten Schlüssel zu erfahren. Andernfalls könnte er die Schlüssel weitergeben und so anderen den Zugang ermöglichen.

Das hier beschriebene Verfahren ist im Bereich Pay-TV weit verbreitet, da dort der gleiche verschlüsselte Datenstrom an viele Nutzer verteilt wird (Broadcasting). Es eignet sich nicht gut für individuelle Informations- und Kommunikationsdienste, die jeweils eine Punkt-zu-Punkt-Verbindung zwischen Dienstanbieter und Dienstnutzer erfordern.

3.3 Kleine Geräte mit individuellem Authentisierungsschlüssel

Ein Mensch erhält bei der Buchung eines Dienstes ein (kleines) Gerät, das einen individuellen Authentisierungsschlüssel enthält. Möchte der Nutzer den Dienst in Anspruch nehmen, sendet er eine Dienstanforderung ab. Der Dienstanbieter fordert den Nutzer auf, sich zu authentisieren, indem er ihm eine sog. Challenge, meist eine Zufallszahl, schickt, die im Gerät mittels einer kryptographischen Einwegfunktion ($y = f(x)$ ist effizient berechenbar, aber $f^{-1}(y) = x$ nicht) und unter Verwendung des individuellen Authentisierungsschlüssels in eine Antwort (Response) umgerechnet wird. Die Response erhält der Dienstanbieter und kann prüfen, ob der Nutzer im Besitz des passenden individuellen Authentisierungsschlüssels ist, ohne diesen selbst übertragen zu müssen. Man spricht deshalb von einem Challenge-Response-Verfahren (Abbildung 9).

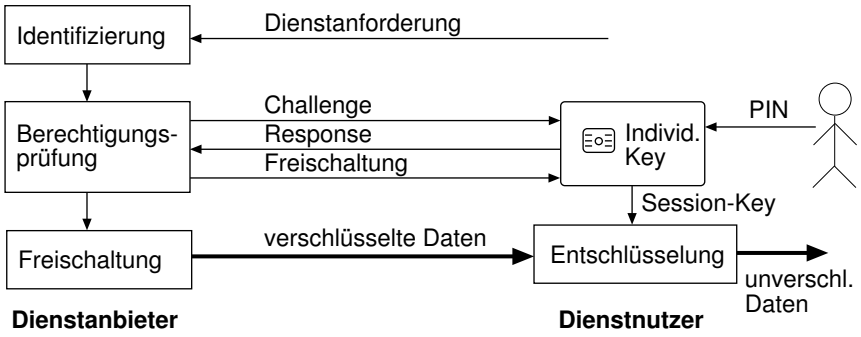

Abbildung 9: Zugangskontrolle mittels Challenge-Response-Authentikation

Bei einem sicheren Verfahren ist es nicht effizient möglich (praktisch unmöglich), aus der Kenntnis von Challenge-Response-Paaren auf den individuellen Authentisierungsschlüssel oder unbekannte Challenge-Response-Paare zu schließen. Ein Abhörer auf der Leitung kann somit keine geheimen Zugangsdaten erfahren. Nach erfolgreicher Authentikation erhält der Nutzer einen Freischaltcode (Sitzungsschlüssel), der nur für begrenzte Zeit gültig ist, mit dem er die übertragenen Daten entschlüsseln kann. Auch hier muss das Gerät physisch so aufgebaut sein, dass der individuelle Authentisierungsschlüssel geheim bleibt. Allerdings liegt die Geheimhaltung im ureigenen Interesse des Nutzers, da es sich um einen „persönlichen“ Schlüssel handelt. Um das Gerät vor Missbrauch nach Verlust oder Diebstahl zu schützen, besitzt es seinerseits einen Zugangskontrolldienst: Über die korrekte Eingabe eines Passworts oder einer PIN wird das Gerät aktiviert.

Die Grundidee des beschriebenen Verfahrens wird beispielsweise bei den SIM-Karten (Subs-

criber Identity Module) von GSM-Mobiltelefonen angewendet. Das Verfahren eignet sich sehr gut für Informations- und Kommunikationsdienste und eingeschränkt für Rundfunkangebote. Es sind hier Verschlüsselungsverfahren mit individuellen Entschlüsselungsschlüsseln (Broadcast-Encryption) bekannt, die jedoch in der Anwendung recht umständlich und ineffizient arbeiten [4, 11]. Sie ermöglichen jedoch bei illegal auftauchenden Schlüsseln eine Rückverfolgung zum ursprünglichen Käufer (Traitor Tracing).

4 Sicherheit von Zugangskontrolldiensten

Die folgenden Abschnitte beschäftigen sich mit der Sicherheit von Zugangskontrolldiensten und deren Anwendung in Rundfunkangeboten sowie Informations- und Kommunikationsdiensten. Zunächst werden grundsätzliche Faktoren der Sicherheit von Zugangskontrolldiensten genannt und anschließend einige Beispiele für Dienste diskutiert.

4.1 Faktoren der Sicherheit

Die Sicherheit der Komponenten von Zugangskontrolldiensten hängt von folgenden Faktoren ab:

- **Angreifermodell:** Bietet das System nur Schutz vor ehrlichen Benutzern oder auch intelligenten Angreifern? Schutz vor intelligenten, bösartigen Angreifern ist deutlich schwieriger zu erreichen als Schutz vor solchen, die sich lediglich im Rahmen der erlaubten und angebotenen (technischen) Möglichkeiten bewegen.

- **Offenheit:** Ist das System für eine offene oder eine geschlossene Umgebung gedacht? Schutz in geschlossenen Umgebungen ist meist deutlich leichter zu erreichen, da man mit deutlich weniger Randbedingungen (z.B. einzuhaltende Standards) konfrontiert ist. Andererseits neigen geschlossene Systeme dazu, weit weniger gut untersucht und geprüft zu sein, weshalb es sich durchaus um eine Scheinsicherheit handeln kann. Offene und sichere Systeme sind stets einsetzbar in einer geschlossenen Umgebung; das Umgekehrte gilt meist nicht.

- **Kapselung:** Ist das System unter Benutzung einer sog. Tamper Resistant Hardware gegen Ausforschung gekapselt oder nur in Software implementiert? Systeme in Hardware erreichen den notwendigen Schutz von Geheimnissen (Dekodierschlüssel) deutlich besser als Softwarelösungen. In Software können Geheimnisse nahezu nicht vor einem intelligenten Angreifer geschützt werden.

- **Plattform:** Wird der Zugangskontrolldienst auf einem speziellen Zielsystem (Dedicated Hardware, z.B. Player-Hardware, Set-Top-Box) oder einem umprogrammierbaren Zielsystem (Multi Purpose Computer, z.B. PC, PDA) ausgeführt? Auf speziellen Zielsystemen (Set-Top-Boxen) sind spezielle ausforschungssichere Hardwarebausteine eher realisierbar,

weshalb nachgeschaltete Softwarelösungen hier einen angemessenen Schutz bieten können. In Universalrechnern (PCs) fehlen bisher solche Hardwarebausteine und müssten vom Inhalte-Anbieter mitgeliefert werden. Allerdings sind selbst spezielle Zielsysteme heute teilweise programmierbar, um Software-Updates realisieren zu können. Dies gilt beispielsweise auch für die im Abonnenten-TV eingesetzte d-box. Ein Angreifer könnte somit über das unberechtigte Updaten einen Zustand erreichen, in dem ein unberechtigter Zugang möglich ist.

4.2 Beispiele für Umgehungsvorrichtungen

Umgehungsvorrichtungen erlauben die Nutzung (Entschlüsselung) eines Dienstangebots unter Umgehung des Zugangskontrolldienstes. Als Umgehungsvorrichtungen sind Computerprogramme zum Mitprotokollieren oder Knacken der Zugangscodes, Manipulationen an den Geräten und der Software zur Zugangskontrolle (Chipkarte, Player, Set-Top-Box) sowie der komplette Nachbau von Hard- und Software unter Umgehung des Zugangskontrolldienstes bekannt.

Im folgenden werden einige Beispiele für bekannte Umgehungsvorrichtungen gegeben.

4.2.1 Modifizierte originale Smartcards

Modified Original Smart Cards (MOSC) sind veränderte, originale Smartcards Anbieters von Abonnenten-TV. Ziel dabei ist es, entweder Karten gekündigter Abonnements zu „reanimieren“ oder Karten mit eingeschränkter Programmnutzungsmöglichkeit von der Einschränkung zu befreien. Bei diesem Angriff werden Smartcards (und insbesondere deren Inhalte) nicht etwa kopiert, sondern verändert.

Im regulären Betrieb empfängt die Smartcard Steuernachrichten (Electronic Control Messages, ECMs), die während des laufenden Programms gesendet werden. Die ECMs dienen zur Aktivierung, Deaktivierung, Funktionserweiterung und Aktualisierung der Nutzungsmöglichkeiten im laufenden Betrieb.

Jede Smartcard besitzt eine eindeutige, 3 Byte lange Seriennummer, mit der sich die Smartcard identifiziert. Durch Senden entsprechender ECMs können so teilnehmerindividuelle Steuernachrichten verschickt werden. So werden beispielsweise für Pay-Per-View-Angebote zur Freischaltung der jeweiligen Sendung teilnehmerindividuelle ECMs gesendet. Von Zeit zu Zeit werden auch die auf der Smartcard gespeicherten Schlüssel aktualisiert (ähnlich einem regelmäßigen Passwortwechsel beim Computer).

Auch der 8 Byte lange Master-Key wird beim offiziellen Freischalten einer Karte gesendet und kann bei der Übertragung leider mitprotokolliert werden, da er unverschlüsselt übermittelt wird. Der Master-Key ist aus Effizienzgründen nicht teilnehmerindividuell, sondern für ganze Kartengruppen gleich. Insofern ist es nicht verwunderlich, dass im Laufe der Zeit Listen mit Master-Keys im Internet veröffentlicht wurden. Kennt man den eigenen Master-Key nicht, weil er beim

Freischalten der Smartcard nicht mitprotokolliert wurde, kann man ihn sehr wahrscheinlich in einer solchen Liste finden.

Jede Steuernachricht, die an die Smartcard gesendet wird, muss mit einem 5 Byte langen Message Authentication Code (MAC, eine Prüfsumme) versehen sein, in den u.a. auch der Master-Key eingeht. Die Spezifikation des kryptographischen Verfahrens zur Berechnung des MAC ist nicht veröffentlicht. Somit wäre es für einen Angreifer normalerweise nicht möglich, gültige Steuernachrichten (z.B. zur Freischaltung nicht bezahlter Sendungen) an die Smartcard zu schicken, da er den passenden MAC nicht kennt.

Leider wurden jedoch bei den ersten Generationen der Smartcard-Software entscheidende Fehler bei der Gestaltung des Kommunikationsprotokolls gemacht. Sobald ein Angreifer eine nicht authentisierte Steuernachricht an die Smartcard schickt, meldet diese erwartungsgemäß einen Authentisierungsfehler, liefert aber überraschenderweise 4 Byte des gültigen MAC zurück. Das fehlende Byte (= 8 Bit) muss anschließend durch Probieren gefunden werden. Hierzu sind maximal 256 Operationen (2^8) notwendig, die wenige Sekunden Rechenzeit benötigen. Bei einem sicheren Verfahren währen jedoch 2^{40} ($= 2^{5 \cdot 8} \approx 10^{12}$) Operationen (Rechenzeit mehrere 10 Jahre) nötig, um den gültigen MAC zu finden. Durch diesen Fehler wurde folglich der Rechenaufwand für den Angreifer etwa um den Faktor 4 000 000 000 gesenkt. Bei der folgenden Kartengeneration wurde die beschriebene Schwäche behoben. Leider konnte aber hier eine Timing Attack (siehe Abschnitt 2.1) auf die Smartcard durchgeführt werden. Man fand heraus, dass sich die Rechenzeit der Karte bei Prüfung des MACs unterscheidet, wenn ein korrektes oder falsches Byte des MACs an die Karte geschickt wird. Somit war es nun möglich, den korrekten MAC Byte für Byte zu ermitteln. Der maximale Gesamtaufwand ist mit $5 \cdot 2^8 = 1280$ Operationen immernoch um etwa den Faktor 860 000 000 niedriger als bei einem sicheren Verfahren.

Mit der Möglichkeit, eine authentische Steuernachricht an die Karte zu senden, war das unberechtigte Freischalten einer Smartcard möglich, indem zunächst die Smartcard in einen am PC angeschlossenen Kartenleser gesteckt wurde, anschließend eine gültige Steuernachricht am PC erzeugt wurde und der entsprechende Steuercode schließlich an die Karte gesendet wurde.

Von Zeit zu Zeit werden vom Sender auch Steuernachrichten ausgestrahlt, die eine MOSC deaktivieren würden. Deshalb wird mit einem sog. Blocker der Strom an Steuernachrichten analysiert und die entsprechenden Nachrichten vor Erreichen der Karte geblockt. Solche Blocker sind entweder als nicht offizielle Patches (Updates von Teilfunktionen einer Software, normalerweise verwendet, um Programmierfehler zu korrigieren) für Set-Top-Boxen möglich oder werden als Hardware-Baustein (z.B. Card-Doubler zum Nutzen mehrerer nicht notwendigerweise modifizierter Smartcards in demselben Kartenschacht) angeboten.

Manche Steuernachrichten (z.B. Befehle zum Schlüsselwechsel) müssen jedoch unbedingt verarbeitet werden, damit die Sendungen weiterhin entschlüsselt werden können. Diese sind dann wieder manuell mit entsprechendem Aufwand in die Karte einzulesen und der Kreislauf beginnt von vorn (Abbildung 10).

Frei verfügbare Anleitungen zum Modifizieren von Karten finden sich beispielsweise unter http://www.moscwizzards.de.vu/ im Internet.

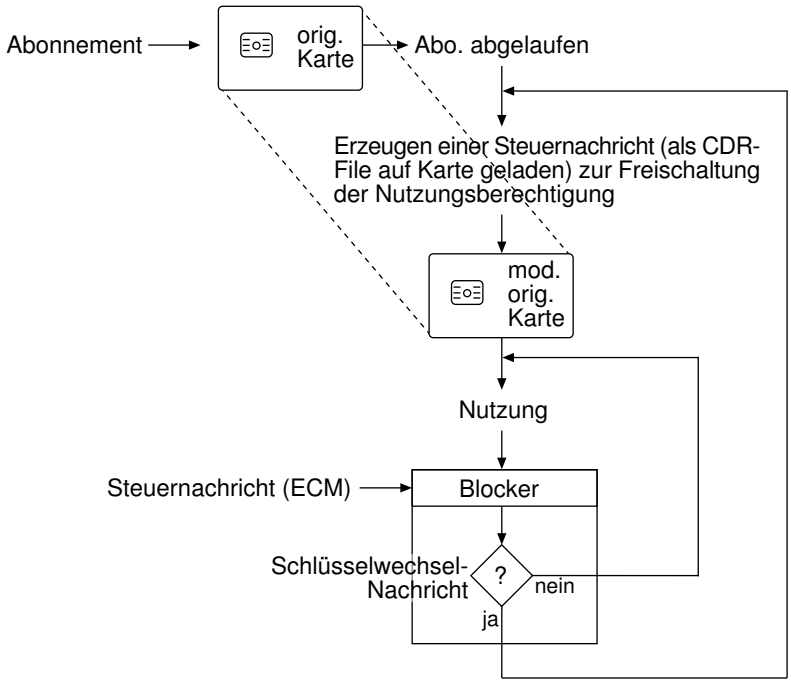

Abbildung 10: Angriffszyklus bei modifizierten originalen Smartcards

4.2.2 Nachbau des Zugangskontrollsystems und Emulation deren Funktion

Sobald man die innere Struktur eines Zugangskontrollsystems durch Reverse Engineering herausgefunden hat, kann man es nachbauen oder seine Funktion nachbilden (emulieren). Normalerweise ist dies gemäß dem Kerckhoffs-Prinzip (Abschnitt 2.2) für den Zugangsschutz selbst nicht problematisch, solange die Geheimnisse (kryptographische Schlüssel) dadurch nicht bekannt werden. Wie in Abschnitt 4.2.1 bereits beschrieben, sind jedoch die Geheimnisse selbst nicht genügend geschützt. Dieser fehlende Geheimnisschutz ist aus technischer Sicht als das Hauptproblem beim Umgehen von Zugangskontrolldiensten einzuschätzen.

Nachbauten von Zugangskontrollsystemen finden sich auch im Bereich des Abonnenten-TV. Die sog. Digital Pirate Smart Cards (DPSC) sind recht teure (einige 10 bis 100 EUR), funktionsgleiche Nachbauten von originalen Smartcards. Natürlich werden von den Piraten nur die notwendigen Funktionen zum unberechtigten Entschlüsseln der Sendungen implementiert. Vereinfacht gesagt werden die Funktionen zur Nutzungsbeschränkung und zum Sperren von Karten einfach weggelassen. Die Herstellung eines solchen Nachbaus ist recht aufwendig, da hierfür spezielle Geräte zur Chipkartenherstellung bzw. Hardwareprogrammierung benötigt werden.

Mit der Verfügbarkeit von programmierbaren Smartcards beschränkt sich der Aufwand eines Piraten auf das Reverse Engineering der Karte und das anschließende „Nachprogrammieren“ deren Funktion in einem Emulator. Der Programmcode wird auf eine entsprechend programmierbare Smartcard geladen, die in der Set-Top-Box wie eine echte Karte arbeitet. Da der Programmie-

rer die Möglichkeit hat, den Funktionsumfang gegenüber einer originalen Karte zu erweitern und zu verändern, kann der Emulator beispielsweise einen Schlüsselwechsel erkennen und verarbeiten. Programmierbare Smartcards sind wegen ihrer universellen Anwendungsmöglichkeiten (Zugangskontrolle zu Gebäuden und Gebäudeteilen, Zeiterfassungssysteme, digitale Signatursysteme, Zahlungssysteme, Mobilfunkanwendungen, Java Card) inzwischen recht preiswert (maximal einige 10 EUR).

In PCs, die über eine digitale Fernsehkarte verfügen, ist es auch möglich, den Emulator als ausführbares PC-Programm zu betreiben. Dieser emuliert dann die Funktion des Conditional-Access-Moduls (CAM) und der Smartcard. Eine weit verbreitete Software hierfür ist z.B. Multidec (http://www.multidec.de/). Multidec selbst ist *keine* Piratensoftware. Sie dient zur Steuerung von PC-Erweiterungskarten für digitales Fernsehen (Digital Video Broadcasting, DVB). Multidec kann allerdings um entsprechende Programmbibliotheken (Soft-CI-DLL) zur Umgehung der Zugangskontrolldienste kostenpflichtiger Angebote erweitert werden. Diese Programmbibliotheken werden im Internet angeboten.

In Abbildung 11 werden die Angriffswege noch einmal graphisch dargestellt.

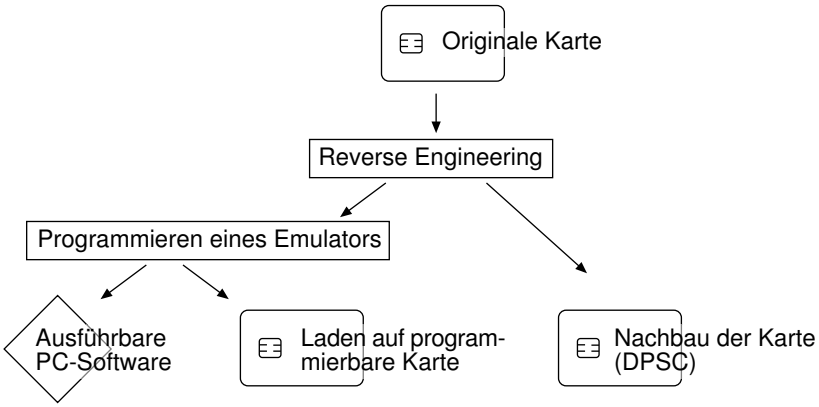

Abbildung 11: Angriffswege beim Nachbau und Emulieren von Zugangskontrollsystemen im Bereich Abonnenten-TV

4.2.3 Digital Rights Management Systeme

Zugangskontrolldienste sind auch Teilsysteme von Digital-Rights-Management-Systemen (DRM-Systeme). DRM-Systeme sind elektronische Vertriebssysteme für digitale Inhalte. Sie ermöglichen die sichere Verbreitung digitaler Inhalte im Online- und Offline-Bereich, z.B. über das Internet, Datenträger, mobile Abspielgeräte oder Mobiltelefone (vgl. [2, S.2ff]).

DRM-Systeme sollen den Rechteinhabern einen sicheren Vertrieb zu berechtigten Nutzern ermöglichen, bieten 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, Abonnement 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.

Ein Anbieter eines Musikstücks könnte beispielsweise das Hineinhören in ein Stück für wenige Cent anbieten, komplettes Hören oder (verschlüsseltes) Speichern auf der Festplatte kostet etwas mehr, übertragen auf einen portablen Spieler oder Brennen auf CD ist deutlich teurer. Solche und ähnliche Angebote werden beispielsweise von den Musikdiensten PressPlay (http://www.pressplay.com/) und MusicNet (http://www.musicnet.com/) angeboten.

Eine Umgehungsvorrichtung könnte nun darin bestehen, eine sehr kostengünstige Lizenz mit eingeschränkter Nutzungsmöglichkeit (z.B. einmal Anhören, nicht abspeichern) um nicht lizenzierte Nutzungsmöglichkeiten zu erweitern (z.B. Brennen auf eine CD). Da es sich bei den Schutzvorrichtungen um reine Softwareobjekte handelt, lassen sich kryptographische Schlüssel unmöglich physisch vor dem ausführenden System (Betriebssystem, PC) schützen. Somit hat ein Angreifer, der das Ausführungssystem (d.h. seinen eigenen PC) entsprechend manipuliert, so dass der Rechner die Inhalte entschlüsselt und unverschlüsselt und frei von Einschränkungen auf die Festplatte speichert, stets die Möglichkeit, rein softwarebasierte DRM-Systeme zu knacken.

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.

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 [5] 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.

Das DRM-System von Digital World Services (http://www.dwsco.com/) ist ebenfalls eine Softwarelösung mit Update-Funktion. Sobald das Schutzsystem geknackt wurde, wird über ein Online-Software-Update wieder die Sicherheit hergestellt.

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.

4.3 Fazit

Zur Umgebung von Schutzvorrichtungen existieren zahlreiche Software-, Hardware- und Informationsangebote.

Eine Umgehungsvorrichtung kann aus vielen unabhängigen Einzelsystemen bestehen, die erst in ihrer für *diesen* Zweck angewendeten Verbindung zu einer Umgehungsvorrichtung wird. Ob deshalb eine bestimmte Person eine Umgehungsvorrichtung besitzt oder nicht, ist deshalb ohne eine konkrete Handlung (Umgehen eines Zugangskontrolldienstes) technisch meist nicht entscheidbar. Ähnliches gilt vermutlich für einen Händler, der Einzelkomponenten verkauft, die auch (aber nicht ausschließlich) in Umgehungsvorrichtungen eingesetzt werden.

Insbesondere Universal-Werkzeuge und Werkzeuge, die neben allgemein nützlichen auch auf das Umgehen von Schutzvorrichtungen spezialisierte Funktionen enthalten, können den (auch völlig unberechtigten) Verdacht erwecken, dass illegale Umgehungsversuche unternommen werden. Beispielsweise kann ein Smartcard-Programmierer auch völlig legal eingesetzt werden. Besonders problematisch wird die Bewertung von Werkzeugen, die nicht nur, aber auch Funktionen zur Umgehung enthalten. Es mag durchaus ein verständlicher Wunsch sein, die legalen Funktionen einer solchen Software zu nutzen, die illegalen aber bewusst zu meiden.

Abschließend muss auch festgestellt werden, dass die erfolgreichen Angriffe auf die Smartcards von Abonnenten-TV-Angeboten leider nicht nur auf die Neugier von technisch interessierten Laien zurückzuführen ist. So schadet es bei einem sicher konzipierten System nicht, wenn ein potentieller Angreifer herausfinden möchte, wie das Schutzsystem funktioniert (Reverse Engineering) und ob es sicher ist bzw. geknackt werden kann. Gerade dieses Interesse eines Angreifers bildet ja die Motivation, Sicherheitsfunktionen in IT-Systeme einzubauen, die nicht leicht, sondern schwer zu überwinden sind. Insbesondere bei der ersten und zweiten Generation der Smartcards wurden jedoch entscheidende Fehler im Design gemacht, die nachher nicht oder nur schwer korrigiert werden konnten. Insbesondere sind dies die fehlende Verschlüsselung bei der Übertragung von Steuernachrichten und deren mangelhafte MAC-Überprüfung.

5 Bewertung des ZKDSG aus technischer Sicht

Im folgenden werden einige Anmerkungen zum Zugangskontrolldiensteschutzgesetz (ZKDSG) aus technischer Sicht gemacht. Die Bewertung unterscheidet sich jedoch durchaus von den juristischen Wertungen in den anschließenden Teilen dieses Buches. Zugangskontrolldienste müssen nicht den aktuellen Stand der Wissenschaft und Technik einhalten, um schutzwürdig zu sein, das

ZKDSG behandelt technisch gleiche Sachverhalte ungleich, und es kann Konsequenzen für die Erforschung von Sicherheitsschwächen in Zugangskontrolldiensten haben.

5.1 Stärke des Zugangskontrolldienstes

Der Gesetzgeber hat mit dem ZKDSG ein technikneutrales Gesetz formuliert, d.h. es finden sich nirgends Aussagen zur konkreten Ausgestaltung des Zugangskontrolldienstes. Außerdem finden sich keine Forderungen nach dem Stand der Technik, auf dem ein Zugangskontrollsystem basieren soll. Wie es auch bei einem Einbruch nicht darauf ankommt, wie gut das aufgebrochene Schloss in der Tür war, so ist auch hier der Unrechtsgehalt nicht geringer, nur weil der Schutz leichter zu überwinden ist. Insofern ist es einem Dienstanbieter möglich, einen schwachen, d.h. leicht überwindbaren, oder völlig veralteten, d.h. z.B. längs geknackten, Zugangskontrolldienst einzusetzen, ohne die eigenen Sorgfaltspflichten zu verletzen.

Einerseits ist es angesichts der schnellen Technikentwicklung verständlich, dass auf konkrete Forderungen bezüglich der konkreten technischen Ausgestaltung des Zugangskontrolldienstes verzichtet wurde. Andererseits ist die Verwendung aktueller Sicherheitstechnologien für einen Anbieter durchaus auch in seinem Interesse. Die entstehenden finanziellen Ausfälle durch erfolgreiche Umgehungsversuche sollten als Anreiz verstanden werden, möglichst gute, ausgereifte Zugangskontrolldienste einzusetzen. Aus der Sicht des Staates ist das nicht unbedingt der Fall: Wenn ein Dienstanbieter aufgrund seines schwachen Zugangskontrolldienstes mit einer Vielzahl von erfolgreichen Umgehungsversuchen (bzw. Vorrichtungen) aufgrund schwacher Schutzmechanismen konfrontiert ist, gelangt der Staat unter Anwendung der Bußgeldvorschriften des § 6 zu zusätzlichen Einnahmen.

5.2 Ungerechtfertigte Ungleichbehandlung gleicher technischer Sachverhalte

Das ZKDSG behandelt technisch gleiche Sachverhalte (Verfahren zur Zugangskontrolle) ungleich, indem manche Zugangskontrolldienste vom Gesetz erfasst werden, andere aber nicht. Auch die Voraussetzung, dass Inhalte verschlüsselt werden müssen, schränkt die Anwendbarkeit des ZKDSG aus technischer Sicht unnötig ein.

5.2.1 Abhängigkeit vom genutzten Kommunikationsdienst

Obwohl der Zweck des ZKDSG ist, Zugangskontrolldienste gegen unerlaubte Eingriffe zu schützen (§ 1), erfasst es nicht alle technischen Systeme, in denen Zugangskontrolldienste eingesetzt werden. Beispielsweise verwenden Computersysteme und -netze, persönliche Kommunikationsdienste (z.B. E-Mail), Mobiltelefone und -netze ebenfalls Einrichtungen zur Zugangskontrolle. Die technischen Komponenten der dort eingesetzten Zugangskontrolldienste unterscheiden sich nicht prinzipiell von denen, die vom ZKDSG erfasst werden: Es wird zunächst die Authentizität

(eines Menschen oder eines Gerätes) überprüft, bevor der Nutzer die Berechtigung zur Dienstnutzung erhält. Selbst einige Kopierschutzsysteme arbeiten nach diesem Prinzip: Durch die korrekte Eingabe eines Freischaltcodes (Authentifizierung durch Wissen, ähnlich einem Passwort) wir die Software zur Nutzung freigeschaltet.

Insofern wird das Knacken bzw. Umgehen ein und derselben Zugangskontrolltechnik, die lediglich für unterschiedliche Dienste eingesetzt werden, unterschiedlich behandelt.

5.2.2 Gebundenheit des ZKDSG an Verschlüsselung

Dass der Einsatz von Verschlüsselung der übertragenen Inhalte eine notwendige Voraussetzung für die Anwendbarkeit des ZKDSG ist, ist technisch gesehen (zumindest in dieser Allgemeinheit) wegen der technischen Unabhängigkeit von Zugangskontrolle und Übertragungsverfahren eine unverständliche Einschränkung.

Es ist durchaus sinnvoll, auch unverschlüsselte, aber zugangskontrollierte und entgeltpflichtige Dienste unter den Schutz des ZKDSG zu stellen. Beispielsweise bieten Access Provider (Internet Service Provider, ISP) öffentliche, aber kostenpflichtige Zugänge zum Internet an. Bei der Einwahl (egal, ob mittels Analog-, ISDN- oder DSL-Modem) authentisiert sich der berechtigte Benutzer gegenüber dem ISP mittels Nutzerkennung und Passwort. Die anschließende Übertragung der Daten (IP-Pakete, wobei egal ist, welcher Internetdienst gerade genutzt wird) geschieht zwischen ISP und Benutzer ohne zusätzliche Verschlüsselung. Eine Umgehungsvorrichtung könnte beispielsweise so arbeiten, dass vom Angreifer im Haus des berechtigten Benutzers das Telefonkabel angezapft wird, um die Nutzerkennung und das Passwort abzuhören.

Allerdings muss erwähnt werden, dass technisch gesehen heute in nahezu allen Anwendungsbereichen eine zusätzliche Verschlüsselung möglich wäre, beispielsweise mittels speziell auf die Anforderungen von ISPs zugeschnittener VPN-Lösungen (Virtuelle Private Netze). Virtuelle Private Netze werden zur Absicherung von Zugriffen von Außen auf organisationsinterne Rechnernetze eingesetzt. Positiv gesagt, kann man die Forderung nach Verschlüsselung der Inhalte natürlich auch als Motivation für die Provider aufzufassen, Verschlüsselung tatsächlich zu implementieren.

Jedenfalls wäre es eine technisch ungerechtfertigte Ungleichbehandlung, wenn passwortgeschütze Internetdienste zwar den Inhalt (beispielsweise kostenpflichtige Downloads von Artikeln, Videos und Musik) verschlüsseln müssten, aber an den eigentlichen Zugangskontrolldienst (Abfrage und Überprüfung des Passworts) keinerlei Forderungen gestellt würden, z.B. das Passwort auch unverschlüsselt übertragen werden darf.

5.3 Konsequenzen für die Erforschung von Sicherheitsschwächen

Bisher war es kaum möglich, die Umgehung von technischen Schutzmaßnahmen juristisch zu verfolgen und zu sanktionieren. Mit der Verabschiedung des Digital Millennium Copyright Act (DMCA) wurden in den USA jedoch Gesetze geschaffen, mit denen ein effekti-

ver juristischer Umgehungsschutz erreicht werden soll. Allerdings sind diese Gesetze umstritten, da sie nicht nur Hackern das Leben schwerer machen, sondern auch dazu geeignet sind, die Freiheit von Wissenschaft und Forschung einzuschränken. So wurde einer Forschergruppe um Prof. Edward Felten von der Universität Princeton nahegelegt, die Veröffentlichung seiner Forschungsergebnisse einer Untersuchung der von der Secure Digital Music Initiative (SDMI) vorgeschlagenen Verfahren zurückzuziehen (siehe http://cryptome.org/sdmi-attack.htm). Der DMCA führte damit auch zur Verunsicherung anderer Wissenschaftler. Der niederländische Kryptograph Niels Ferguson beispielsweise soll im Juli 2001 einige Schwächen von Intels Digital-Rights-Management-Technologie HDCP (High-bandwidth Digital Content Protection, siehe http://www.digital-cp.com/) aufgedeckt haben, sagt aber, er habe sich entschieden, diese nicht zu publizieren, sondern für sich zu behalten, da er andernfalls mit einer Anklage und einem Gerichtsverfahren zu rechnen habe [9].

Obwohl das ZKDSG eindeutig nur ein Verbot von gewerbsmäßigen Handlungen vorsieht, so ist nicht auszuschließen, dass auf Personen, die sich beruflich mit dem Testen und Verbessern von IT-Sicherheitsmechanismen beschäftigen, der Druck wächst, ihre Ergebnisse nicht zu publizieren. Hierdurch könnte die Gefahr entstehen, dass längst bekannte Umgehungsmöglichkeiten nicht rechtzeitig beseitigt werden, wodurch zusätzlicher Schaden für die Dienstanbieter entstehen würde. Dies würde jedoch dem Ziel des Gesetzes (Verhindern des kostenlosen Erschleichens der Nutzung) zuwiderlaufen.

Weiterhin ist nicht auszuschließen, dass seriös publizierte Umgehungsmöglichkeiten, die aufgrund prinzipieller Schwächen eines Zugangskontrollsystems nicht einfach abgestellt werden, von gewerbsmäßig motivierten Anbietern von Umgehungsvorrichtungen implementiert werden und dem Entdecker der Schwäche eine entsprechende Mitverantwortung angelastet wird. All dies könnte zu einer faktischen oder empfundenen Einschränkung der Forschungsfreiheit führen.

6 Zusammenfassung

Zugangskontrolldienste dienen dem Schutz kostenpflichtiger, an die Allgemeinheit gerichteter, verschlüsselter Rundfunkangebote und Teledienste.

Ein Zugangskontrolldienst muss nicht dem Stand der Technik entsprechen, um nach dem ZKDSG schutzwürdig zu sein. Jedes gewerbsmäßige Handeln bei der Umgehung von solchen Schutzvorrichtungen ist verboten, egal ob der Zugangsschutz trivial oder nur sehr aufwendig zu umgehen ist.

Beispiele für bekannte und erfolgreiche Umgehungsmöglichkeiten für Zugangskontrolldienste sind:

- Softwaredecoder für analoges und digitales Abonnenten-TV,
- Piratenkarten (entweder Nachbauten von Originalen oder entsprechend programmierte Universalkarten) für digitales Abonnenten-TV,

- Modifizierte Originalkarten, die nach einer abgelaufenen Nutzungsberechtigung „reanimiert“ werden oder um nicht bezahlte Nutzungsberechtigungen erweitert werden,
- Programme zum Protokollieren und/oder zeitnahen Knacken von Medienschlüsseln verschlüsselter Inhalte sowie zum Blockieren von Steuernachrichten, die der Deaktivierung von Piratenkarten und modifizierten Originalkarten dienen,
- Updates von Playersoftware und Betriebssoftware von Set-Top-Boxen mit dem Ziel, die unbezahlte Nutzung zu ermöglichen oder die Nutzungsmöglichkeiten zu erweitern.

Auch die moderneren Schutzsysteme beim Abonnenten-TV werden trotz ihrer Kompliziertheit meist nach kurzer Zeit geknackt. Dies hat aus technischer Sicht wenigstens folgende Ursachen:

1. Die Schutzsysteme weisen noch aus ihrer Einführungszeit stammende Fehler bzw. Schwächen im Design auf, die aufgrund der weiten Verbreitung nicht mehr kostengünstig abgestellt werden können.
2. Selbst wenn das Design völlig fehlerfrei wäre, müsste man für ein auf absehbare Zeit sicheres Zugangskontrollsystem voraussetzen können, dass auch die physische Sicherheit der Geräte (hier insbesondere der Smartcards) auf absehbare Zeit gewährleistet ist. Dies ist jedoch angesichts der immer wieder bekannt werdenden Schwächen von Chipkarten eine Illusion.

Aus technischer Sicht ist die Ungleichbehandlung gleicher technischer Sachverhalte unverständlich. So fällt das Knacken der Smartcard beim Abonnenten-TV unter das ZKDSG, das Brechen der ebenfalls Smartcard-basierten und funktional gleichwertigen Zugangskontrolle eines Mobiltelefons jedoch nicht.

Literatur

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

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

[3] Alex Biryukov, Adi Shamir, David Wagner: Real Time Cryptanalysis of A5/1 on a PC. In: Proc. Fast Software Encryption Workshop 2000. New York City, 10.–12. Apr. 2000. http://cryptome.org/a51-bsw.htm.

[4] 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.

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

[6] 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/.

[7] 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.

[8] 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.

[9] Stefan Krempl: Kryptologen klagen über massive Forschungsbehinderungen. Heise-News. http://www.heise.de/newsticker/data/jk-30.01.02-012/.

[10] 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.

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

[12] 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.

[13] Sergei Skorobogatov, Ross Anderson: Optical Fault Induction Attacks. In: Proc. Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), Lecture Notes in Computer Science. Springer-Verlag, Berlin, San Francisco, CA, USA, 13.–15. Aug. 2002.

Abkürzungsverzeichnis

A3	Authentisierungsalgorithmus im GSM
A5	Verschlüsselungsalgorithmus im GSM
AES	Advanced Encryption Standard
CAM	Conditional Access Modul
CD	Compact Disc
CI	Common Interface
DES	Data Encryption Standard
DLL	Dynamic Link Library
DRM	Digital Rights Management
DMCA	Digital Millennium Copyright Act
DNA	Deoxyribonucleic acid (Desoxyribonucleinsäure)
DPSC	Digital Pirate Smart Card
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
ECM	Electronic Control Message
GSM	Global System for Mobile Communication
HBCI	Home Banking Computer Interface
HDCP	High-bandwidth Digital Content Protection
HTTPS	Secure HTTP
HTTP	Hypertext Transfer Protocol
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Informationstechnik
MAC	Message Authentication Code
MOSC	Modified Original Smart Card
MP3	MPEG Audio Layer 3
MPEG	Moving Picture Experts Group
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RSA	Rivest, Shamir, Adleman (Erfinder von RSA)
SDMI	Secure Digital Music Initiative
SIM	Subscriber Identity Module
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TV	Television
URL	Uniform Ressource Locator
VPN	Virtual Private Network
ZKDSG	Zugangskontrolldiensteschutzgesetz

Index