Semesterarbeit zu dem Thema:

Premiere BetaCrypt (Irdeto)
Das (alte) dedizierte Verschlüsselungsverfahren auf der D-BOX

Hochschule Bremen ~ Labor für Computertechnik
Wintersemester 2004 / 05

Vorgelegt von: Dany Drygalla
Andreas Haase

Hochschullehrer: Prof. Dr. Th. Risse

1 Inhaltsverzeichnis

2 Abbildungs- und Tabellenverzeichnis

3 Einführung – Überblick [1]

3.1 Geschichte des Bezahlfernsehens in Deutschland

Zu Beginn der neunziger Jahre gab es nur einen einzelnen analogen Pay-TV – Kanal in Deutschland. Dieser Kanal war mit dem Verfahren Nagravision I (SYSTER) verschlüsselt. Die „Verschlüsselung“ basierte im Prinzip auf einer zufälligen Vertauschung von normalerweise aufeinander folgenden Bildzeilen. Der Ton wurde noch unverschlüsselt übertragen.
Die nötigen Decoder gab es nicht auf dem freien Markt zu kaufen; Sie waren nur über Fernseh-Fachhändler zur Miete erhältlich.
Doch war es im Laufe der Zeit (ca. 1998) mit immer leistungsfähigeren und PCs (etwa ab dem Leistungsniveau eines Intel Celeron Prozessors mit 400Mhz und 64MB SDRAM) für den Privatanwender möglich, die Verschlüsselung durch Analyse des verschlüsselten Bildes mit illegal erhältlicher Software in Echtzeit zu umgehen. Die Entwickler machten sich dabei die Tatsache zu nutze, dass ein unverschlüsseltes Fernsehbild als Ganzes zwar viele unterschiedliche Informationen beherbergt, benachbarte Zeilen jedoch nahezu identische Informationen (Helligkeit, Farbe) enthalten. Die Software analysierte diese Zeileninhalte und konnte dadurch die Bildzeilen wieder in die richtige Reihenfolge bringen. Dieses „Sortieren“ konnte umso besser gelingen, je mehr unterschiedliche Informationen das Bild selbst enthielt. Im Umkehrschluss bedeutet dies, dass der „Sortier-Algorithmus“ jedoch Schwierigkeiten bei Fernsehbildern hatte, die als Ganzes nur wenig Unterschiede enthalten, z.B. der Rasen auf dem Fußballfeld, eine dunkle Szene in einem Film oder der Abspann bei Kinoverfilmungen.
1996 wurde der erste digitale Fernsehsender, DF1, von der Kirch-Gruppe ins Leben gerufen. Die im Vorfeld massiven Marketing-Maßnahmen stießen bei den Verbrauchern zu diesem Zeitpunkt jedoch nur auf geringe Resonanz. Das Verschlüsselungssystem basierte auf „IRDETO“.
Als Antwort auf die vielen „analogen Schwarzseher“ startete Premiere, zunächst im parallelen Betrieb mit dem analogen System Nagravision, sein digitales Fernsehprogramm. Zahlende „analoge Kunden“ sollten unterdessen zu günstigen Konditionen auf den Umstieg zu Premiere Digital bewegt werden.

Im Jahr 1999 übernahm Premiere DF1 und dessen Verschlüsselungssystem „IRDETO“. Premiere hatte jedoch auch finanzielles Interesse daran, seine eigenen Digital-Receiver zu vertreiben, mit denen nur Premiere und die „Free-To-Air“ Programme empfangbar sein sollten. Mit dem reinen IRDETO wäre dies jedoch nicht möglich gewesen, da es bereits einige Receiver auf dem freien Markt gab, die IRDETO unterstützten. Anders herum hätte ein Kunde die Möglichkeit, den Receiver von Premiere für andere (evtl. zukünftige) Pay-TV Anbieter einzusetzen, wenn diese ebenfalls die IRDETO -Verschlüsselung lizensierten. Deshalb wurde IRDETO von einer Tochtergesellschaft, BetaResearch, zu BetaCrypt modifiziert. Es gibt jedoch einige IRDETO - Receiver auf dem Markt, die auch in der Lage sind, BetaCrypt zu dekodieren.

[1] http://www.iswitch.ch/ma.pdf

4 Analoge Verschlüsselungsverfahren [2]

Die Zeit des analogen Fernsehens neigt sich dem Ende zu. In der Welt des Satellitenfernsehens geschieht dies viel schneller, als für den Zuschauer am Kabelanschluss. Mit dem Wegfall des analogen Fernsehens verschwinden auch die analogen Verschlüsslungssysteme, da diese für digitale Übertragungen nicht mehr gebraucht werden können. Im Gegensatz zu digital codierten Übertragungen, wo man nur einen schwarzen Bildschirm sieht, kann man bei analog codierten Übertragungen das codierte Bild tatsächlich sehen. Es drängt sich die Frage auf, wieso man ein digital gesendetes Bild nicht einfach analog codiert überträgt. Der Grund liegt im Bildkompressionsverfahren MPEG2, welches bei digitalen Übertragungen eingesetzt wird. MPEG2 verändert das Bild für den Menschen zwar nur unscheinbar, für die analogen Decoder hingegen, gehen wichtige Informationen verloren, die eine entschlüsselte Darstellung eines digital komprimierten und analog codierten Bildes unmöglich machen. Bei analogen Verschlüsslungssystemen ist es üblich, dass nur das Bild verschlüsselt wird. Den Ton kann man selbst ohne den entsprechenden Decoder hören. Obwohl analoge Verschlüsslungsverfahren heute praktisch keine Rolle mehr spielen, haben sie vor einigen Jahren noch eine große Verbreitung gehabt. Dabei wurden in Europa vor allem drei Systeme eingesetzt: Eurocrypt (vorwiegend in Skandinavien), Nagravision/Syster (Deutschland/Frankreich u.a.) und Videocrypt I/II (Großbritannien).

4.1 Beispiel Nagravision / Syster [3]

Hierbei handelt es sich um eine Schweizer Entwicklung aus dem Hause Kudelski. Das System arbeitet mit Zeilenvertauschungen. Bei Nagravision werden die Zeilen eines Halbbildes nach einem bestimmten Schema vertauscht (lineshuffling). Bei einem Beispielbild von 16 Zeilenblöcken, sind bei diesem Verfahren 32768 (2^{n-1} è $2^{16-1} = 2^{15}$) verschiedene Zeilenpermutationen möglich. Das System holt die Informationen auch aus der Austastlücke und decodiert über eine Smartcard. Allerdings ist Nagravision das wohl am einfachsten zu knackende System überhaupt. Dabei ist weder die Smartcard noch der Decoder an sich notwendig. Es genügt ein Sat- Receiver (bei Kabelempfang entfällt auch dieser) und ein Computer mit einer analogen TV- Karte. Der Rechenaufwand bei Decodierung von Nagravision auf dem Computer ist um ein Vielfaches geringer als bei Videocrypt. Es wird dabei eine annähernd perfekte Bildqualität erzielt.

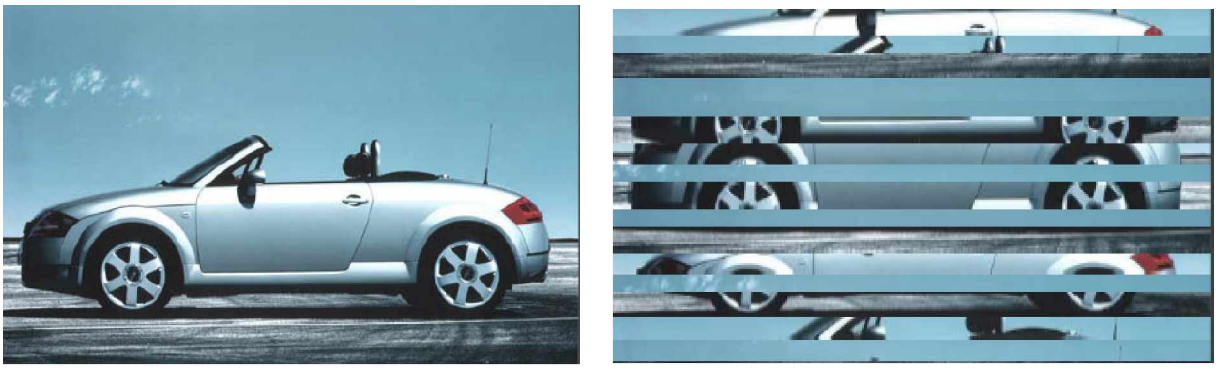

Abbildung 1: Beispiel: Nagravision Verschlüsselung (Syster) mit 16 Zeilenblöcken

[2] http://www.imn.htwk-leipzig.de/%7Edittmann/vorles-mm-02-studenten-folien-2perpage-1.pdf, Seite 64 ff

[3] http://www.cl.cam.ac.uk/~mgk25/nagra.pdf

Die Vorgehensweise des PC-Decoderprogramms ist einfach:
Es sucht im verschlüsselten Halbbild nach auseinander liegenden Bildzeilen, die im unverschlüsselten Halbbild nebeneinander liegen könnten. Findet es solche, dann führt die entsprechende Vertauschung dieser Position zum richtigen Bildteil.
Es müssen natürlich mehrere Zeilen analysiert werden, um festzustellen, ob eine vermutete Permutation auch die richtige ist. Analysiert werden im eigentlichen Sinne z.B. die Luminanz der einzelnen Bildpixel: Ist die Luminanzdifferenz klein, so ist es wahrscheinlich, dass die Zeilen beieinander liegen. Damit diese Methode funktioniert, bedarf es gewissen Voraussetzungen beim Fernsehbild: Nahe bei einander liegende Zeilen müssen eine ähnliche, weiter entfernte eine unterschiedliche Luminanz haben. Dies führt bei der Decodierung von Übertragungen von z.B. Fußballspielen zu Problemen, da dort praktisch das gesamte Bild grün ist.

4.2 Eurocrypt

Die Eurocrypt-Verschlüsselung wird nur auf in D2MAC gesendete Signale eingesetzt. D2MAC (MAC = Multiplex Analog of Components) ist ein „halbdigitales“, hochwertiges Fernsehsystem, welches auf PAL aufbaut. D2MAC ist die neuste Version der MAC-Entwicklungsreihe (A-MAC, B-MAC, C-MAC, D-MAC). D2MAC wurde speziell für den Einsatz bei Satellitenübertragungen entwickelt. Es ist in einigen Punkten dem konventionellen PAL-System überlegen:

- Bessere Nutzung der Satelliten- Signalstärke
- Digitale Audio-Übertragung (Nicam-Stereo)
- Übertragung zusätzlicher Dienste (z.B. Untertitel, Videotext, Eurocrypt)
- 16:9-Darstellung möglich
- Größere Video-Bandbreite ermöglicht bessere Bildgenauigkeit/-schärfe

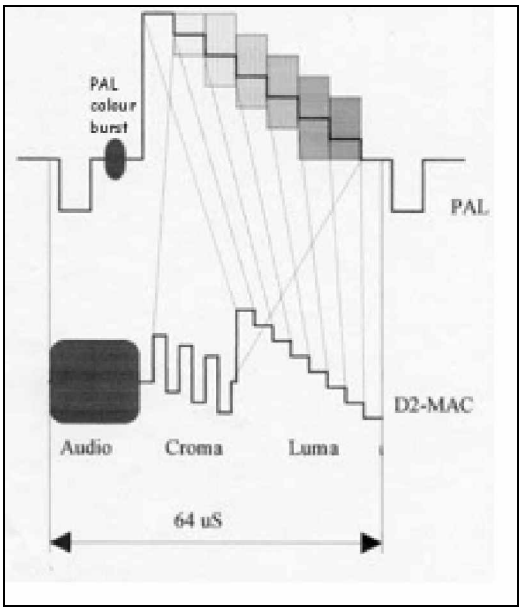

Abbildung 2: Theoretische Aufzeichnung eines PAL/D2MAC Signals

Dabei macht sich D2MAC die so genannte Time Division Multiplexing-Technologie zu Nutze. Wie in der Grafik zu sehen ist, werden dabei Audio, Chrominanz und Luminanz nacheinander, statt gleichzeitig, wie bei PAL, übertragen.

Zurzeit werden noch zwei Unterarten von Eurocrypt verwendet: Eurocrypt-M und Eurocrypt-S2. Bei letzterer kommt eine 56-bit DES Verschlüsselung zum Zug. Die neueste Entwicklung Eurocrypt-S3 (mit 168-bit Triple-DES) wird seit der Abschaltung des analogen Canal+ -Signals nicht mehr verwendet.

Eurocrypt bildete dann später in gewissen Aspekten die Grundlage für das digitale Verschlüsselungssystem Viaccess.

Die Funktionsweise des Eurocrypt-Systems ist seit langer Zeit bekannt. Dies hat dazu geführt, dass die zum Empfang benötigten DES-Schlüssel und die weiteren benötigten Codes geknackt wurden. Derzeit gibt es aber nur noch eine kleine Anzahl Programme, die in D2MAC senden, so dass Eurocrypt nicht mehr weiter interessant ist.

4.3 Videocrypt I /II

Die Videocrypt Verschlüsselung vollzieht sich auf der Ebene der Bildzeilen. Jede einzelne Bildzeile wird mehr oder weniger zufällig an einem von 256 möglichen Punkten in zwei Stücke zerhackt und verschoben. Zusätzlich werden diese Codierungsdaten verschlüsselt in der Austastlücke des Bildes mit gesendet. Diese ist Teil des Fernsehbildes, auf dem Fernseher jedoch nicht sichtbar. In der Austastlücke werden auch andere Daten, wie zum Beispiel Videotext übertragen. Ist ein Videocrypt-Decoder an den Sat-Receiver angeschlossen, erkennt dieser die Videocrypt- Daten der Austastlücke und sendet diese an die eingesteckte Smartcard weiter. In der Smartcard werden die Daten dann durch einen Algorithmus entschlüsselt und dann an den Decoder zurückgeleitet, der die Bildzeilen dann wieder an den richtigen Ort verschiebt. Die beiden Systeme Videocrypt I/II unterscheiden sich nur geringfügig durch interne Codierungsmechanismen voneinander. Die meisten Decoder konnten VC1 und VC2 decodieren. Es existierte noch eine dritte Form von Videocrypt namens SoftVideocrypt. Programme, welche nur softcodiert gesendet wurden (der bekannteste war wohl Channel 5 auf Astra) bedurften keiner Smartcard, um decodiert zu werden. Ein VC-Decoder allein reichte schon.
Das Videocrypt-System wurde eigens von Rupert Murdochs Imperium BSkyB entwickelt und für dessen Programmplattform verwendet.

Im Laufe der Zeit wurde das System mehrmals geknackt, aber immer wieder durch neue Kartengenerationen neu abgesichert. Zuletzt galt das System als sicher. Die einzige Angriffsmöglichkeit stellte dann noch eine Brute-Force-Attacke dar, welche aber eher schlechte Bildqualität erzielte und dazu auch nur wenige Bilder pro Sekunde erzeugen konnte. Die Abschaltung des letzten Transponders des analogen Sky- Programms auf Astra bedeutete auch das Ende von Videocrypt.

Abbildung 3: Videocrypt verschlüsseltes Bild

5 Digitale Verschlüsselungsverfahren [4]

5.1 Allgemeines

5.1.1 DVB

Das DVB-(Digital Video Broadcasting-) System ist derzeit der weltweit akzeptierte Standard für die digitale Übertragung von Fernseh- und Radiosendungen sowie sonstigen Daten, z.B. „Internet per Satellit“. Dieser Standard beschreibt im Wesentlichen, welche Modulationsverfahren auf physikalischer Ebene in Abhängigkeit des Übertragungsweges angewendet werden. Durch die Anwendung unterschiedliche Modulationsverfahren soll sichergestellt werden, dass für unterschiedliche Übertragungswege jeweils die optimale Übertragungsqualität und Datenrate verfügbar ist.

Die Video-Signale werden digitalisiert nach MPEG-2. Besonderes Kennzeichen von digitalen Video-Netzen ist, dass die Daten in Blöcken oder Containern (Transport Stream (TS) Pakete) übertragen werden. Dazu dienen die MPEG-2-Transport-Ströme. Dabei werden Blöcke à 188 Bytes gebildet. Die ersten 4 Bytes davon fungieren als Synchronisations-Byte (Wert 47h), als Meldebits für Fehler, ob die Nutzdaten (auch Payload genannt) verschlüsselt sind und für die Kennzeichnung des Paketes (13 bit PID).

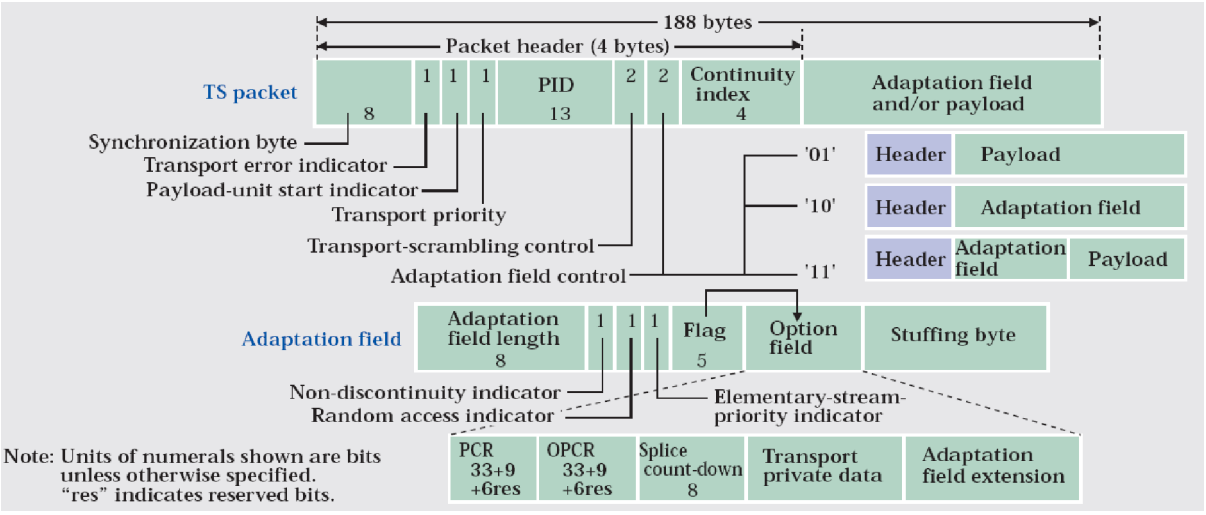

Abbildung 4: Blockschaltbild eines DVB Transport Stream (TS) Paketes

Wesentliche Kennzeichen der digitalen Video-Signale sind:

- durch Komprimierung stark reduzierte Datenrate (von 166 Mbps auf 4 Mbps)
- Übertragung als Transport-Ströme, in 188 Byte langen Blöcken
- Multiplexen, d.h. Zusammenbringen verschiedener Programme *(in einen Transportstrom, Anm. des Autors*), bestehend aus Bild, Ton und Daten
- logische Trennung der Kanäle mittels Packet Identifier (PID)

[4] http://www.tjaekel.de/dvb.htm, 2005-01-23

5.1.2 Conditional Access System [6]

Conditional-Access-Systeme (im Folgenden CAS genannt) werden zum Dekodieren von Programminhalten beim digitalen Fernsehen auf Kundenseite eingesetzt, um eine selektive Entschlüsselung bezüglich einzelner Sender(-gruppen) und Zuschauer zu ermöglichen. Diese CA-Systeme bilden die Schnittstelle zwischen dem verschlüsselten DVB-Datenstrom und der Smartcard des Benutzers (oder Abonnenten). Sinn und Zweck jedes dieser Systeme ist es, ein gültiges acht Byte langes Kontrollwort (CW) zu generieren, das den Datenstrom (Die Nutzlast (Payload) im Transport Stream Paket, Anm. des Autors) entschlüsselt. Verschlüsselt wurde vorher immer mittels des so genannten Common-Scrambling-Algorithmus [8].

Unabhängig vom verwendeten CA-System, muss sich zur Entschlüsselung immer ein eindeutiges CW ergeben. Das ermöglicht unter anderem die Verwendung von mehreren CA-Systemen zur Entschlüsselung ein und desselben Datenstroms (Simulcrypt). Der eigentliche Dekodierungsvorgang erfolgt dann unabhängig vom verwendeten CA-System. Dieser Aufbau ist nötig, um die Empfangsgeräte (auch Receiver) unabhängig vom eingesetzten CA-System bauen zu können. Das verwendete Verfahren wird dann mittels eines Conditional-Access-Modul (CAM) in den Receiver eingesetzt. Die etablierte Schnittstelle für CAMs ist das Common Interface. Die Smartcard, die der Kunde von seinem Anbieter erhält, wird dann entweder direkt in das CAM eingeschoben, oder in einen Kartenleser, der mit dem CAM in direkter Verbindung steht. Das CAM hat die Form und Baugröße einer PCMCIA-Karte, findet sich aber auch als Softwarevariante oder als fest eingebaute Hardwarelösung (zum Beispiel in der D-Box als ASIC, Anm. des Autors).

Zusätzlich zur Information, die sich schon auf der Karte des Kunden befindet, senden alle diese Verfahren noch Steuercodes über den eingehenden Datenstrom. So ist ein eigener Teilbereich (PID) reserviert, mittels denen der Anbieter neue Schlüssel an die Kundenkarten verteilen bzw. Kundenkarten aktivieren oder deaktivieren kann. Diese Steuercodes werden mit Entitlement Management Messages (EMM) und Entitlement Control Messages bezeichnet. Mit diesen Steuercodes wird das vom Anbieter verschlüsselte Control Word für den CSA-Descrambler zum Decoder übermittelt. Das Control Word muss verschlüsselt zum CA-System übertragen werden. Ansonsten ließe sich dieses Control Word in einem modifizierten Decoder filtern und unter Umgehung des CT-Systems zum Descrambler leiten. Die Steuercodes dienen ebenfalls der Fernkonfiguration des Conditional Access Systems, bzw. der Smartcard und werden in 5.1.4 und 5.1.5 genauer beschrieben.

---

[6] http://de.wikipedia.org/wiki/Conditional_Access_System, 2005-01-25

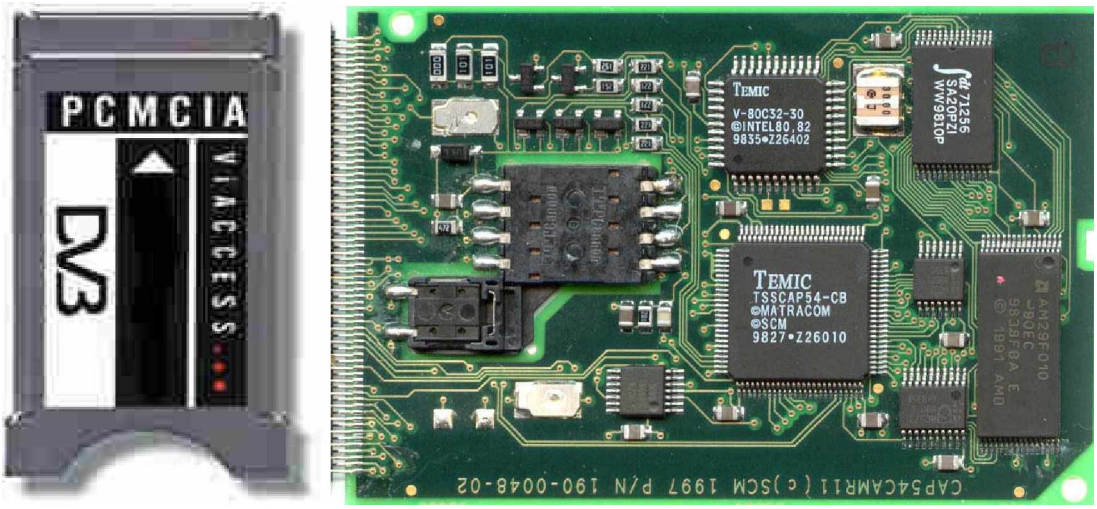

Abbildung 5: VIACCESS CAM Modul

5.1.3 Smartcard

Die Smartcards entsprechen der Beschreibung im ISO7816 Standard.
Die Smartcard ist eine so genannte asynchrone Ausführung im Scheckkartenformat. Diese Karten besitzen einen Mikroprozessor sowie einen EEPROM als Datenspeicher. Asynchron bedeutet, dass auf die im EEPROM der Karte gespeicherten Daten nur über den Mikroprozessor zugegriffen werden kann. Durch diesen Kontrollmechanismus sind die sensiblen Daten auf dem EEPROM der Karte vor fremden Zugriffen geschützt. Der Mikroprozessor enthält Kryptographische RSA- und DES- Einheiten, mit deren Hilfe chiffrierte, per Steuercode eingehende Daten, insbesondere neue Schlüssel, entschlüsselt im EEPROM abgelegt werden.

Die Smartcard dient im CA-System als Dekodierkarte für die in den Steuercodes enthaltenen Daten und enthält mehrere Schlüssel:

- einen signierten Plain Master Key (PMK). Mit Hilfe dieses Schlüssels dechiffriert die Smartcard neue
- Service Keys

Üblich sind bis zu zehn Service Keys im EEPROM der Smartcard. Mit Hilfe eines gültigen Service Keys entschlüsselt der Mikroprozessor auf der Smartcard das Control Word für den CSA-Descrambler.

Warum aber zehn Schlüssel, wenn doch ein einziger Service Key zum Entschlüsseln des Control Words genügt? Die Service Keys stellen konkret die primäre Berechtigung für einzelne Services dar (Ein gültiger Schlüssel berechtigt grundsätzlich zum Empfang eines Services (zum Entschlüsseln des Control Words), deshalb der Ausdruck Service Key). Ein Service bedeutet konkret ein einzelnes Programm oder eine Gruppe von Programmen eines Anbieters. Gibt es nur einen generischen Service Key zum Entschlüsseln aller Control Words, wären also entweder alle Programme eines Anbieters empfangbar oder gar keins, wenn der Schlüssel ungültig ist. Z.B. eine Technik wie Pay per view lässt sich damit nicht sinnvoll umsetzen, da hier der Service Key nur zur Laufzeit der vorbestellten Sendung gültig sein darf. Die Vergabe verschiedener Service Keys ermöglicht dem Anbieter erst, Programm-Pakete mit unterschiedlichem Umfang (und Preisen!) dem Kunden zur Verfügung zu stellen.

5.1.4 Entitlement Management Messages

Mit EMMs werden

- ein einzelner Decoder oder eine Gruppe von Decodern adressiert
- Berechtigungen zum Empfang von einzelnen Kanälen eines Anbieters entzogen oder vergeben
- die Smartcard aktiviert oder gesperrt
- neue gültige Service Keys auf die Smartcard geschrieben. Mit Hilfe der Service Keys entschlüsselt der Mikroprozessor auf der Smartcard das Control Word für den CSA-Descrambler.

EMMs werden über je einen gesonderten logischen Kanal (PID) im Transport Stream zu der Smartcard im Decoder übermittelt. Die PIDs von EMMs werden in einer so genannten Conditional Access Table verwaltet, die jeder Decoder nach dem Einschalten aufbaut. Die Einträge für die Conditional Access Table werden vom Anbieter ebenfalls durch einen gesonderten logischen Kanal im Transport Stream mit PID 0x01h übertragen. Die EMMs sind chiffriert und werden mit Hilfe des so genannten Plain Master Key (PMK) vom Mikroprozessor auf der Smartcard entschlüsselt. Dieser Schlüssel befindet sich nur auf der Smartcard. Würden EMMs im Klartext übertragen, ließen sich sämtliche EMM-Steuercodes genau wie die Service Keys aus dem Transport Stream auslesen. Sind diese bekannt, können sämtliche Steuercodes mit Hilfe eines am PC angeschlossenen Kartenlesegerätes und entsprechender Software emuliert werden. Eine gesperrte Karte wäre dann in Sekunden wieder freigeschaltet bzw. mit neuen gültigen Service Keys ausgestattet.

5.1.5 Entitlement Control Messages

ECMs enthalten

- das für ein Programm aktuell gültige Control Word für den CSA-Descrambler
- Nummer des Service Keys, mit dem das aktuell gültige Control Word entschlüsselt werden muss.
- Datumsstempel

Wie die EMMs werden auch die ECMs über einen gesonderten logischen Kanal (eigener PID) im Transport Stream übertragen. Die PIDs für die ECMs werden ebenfalls in der Conditional Access Table verwaltet.

5.1.6 Common Scrambling Algorithmus (CSA)

Der Common Scrambling Algorithmus (kurz: CSA) ist das Verschlüsselungsverfahren, welches beim Digitalfernsehen DVB verwendet wird, um den Videodatenstrom zu verschlüsseln.
CSA wurde über mehrere Jahre geheim gehalten. Einige Hinweise kamen über die Patentschrift ans Licht der Öffentlichkeit, wichtige Details blieben jedoch geheim, zum Beispiel der Aufbau der so genannten S-Boxen. Ohne diese Details war eine freie Implementierung des Algorithmus' nicht möglich. CSA sollte ursprünglich nur in Hardware implementiert werden, womit es unmöglich schien, die nötigen Details durch Reverse Engineering existierender Implementierungen, zum Beispiel Conditional Access Module (kurz: CAM), zu ermitteln.

Im Jahre 2002 erschien ein Programm namens FreeDec, welches den CSA in Software implementierte. Das Programm war nur als binäre Version verfügbar. Hacker disassemblierten die Software und ermittelten damit die fehlenden Details. Dadurch wurde es möglich, eine Implementierung von CSA in einer Hochsprache zu verwirklichen.
Seitdem der Algorithmus für CSA vollständig bekannt ist, suchen Kryptoanalytiker nach Schwachstellen des Verfahrens. Wie auch bei anderen Verschlüsselungsverfahren ergibt sich ein Angriffspunkt dadurch, dass Teile des Klartextes als bekannt oder zumindest als sehr wahrscheinlich anzunehmen sind (zum Beispiel MPEG-Header). Aus der Länge des Schlüssels (hier: Control Word) von 64 Bit ergeben sich 2^64 Möglichkeiten der Verschlüsselung. Würde man alle möglichen Schlüsselworte mit Hilfe eines Computers durchprobieren, und dieser für jeden Versuch 1 µs benötigen, würde die Suche über 500.000 Jahre dauern. Durch Annahme bestimmter Klartextbytes lassen sich Rückschlüsse auf den verwendeten Schlüssel ziehen, um die Gesamtanzahl möglicher Schlüssel deutlich zu reduzieren.
Sollte es durch Kryptoanalyse möglich sein, den verwendeten Schlüssel durch Kenntnis der Klartextstruktur zu "erraten", wäre CSA geknackt und würde sämtliche Conditional Access Systeme unbrauchbar machen. Dies ist bis heute nicht der Fall. Man bezeichnet dies auch als „Streamhack“.[9]

Die Verschlüsselung des CSA besteht im Prinzip aus einer logischen XOR-Verknüpfung der zu verschlüsselnden Datenbytes mit einer Pseudozufallszahlenfolge. Die Pseudozufallszahlenfolge wird von einer Finite State Machine (FSM) erzeugt, wobei das vom darüber liegendem Conditional Access System gelieferte acht Byte lange Control Word (CW) den Startzustand der FSM festlegt. Auf die Details des CSA soll im Rahmen dieser Arbeit nicht weiter eingegangen werden. Der interessierte Leser findet eine detaillierte Beschreibung sowie zwei mögliche Angriffe auf den CSA-Algorithmus unter

http://www.informatik.tu-darmstadt.de/KP/publications/04/csa_04.pdf

5.2 Irdeto / Betacrypt[10]

Irdeto bzw. Betacrypt ist wohl für den deutschsprachigen Raum das interessanteste Verschlüsslungsverfahren, da dieses beim Programmanbieter Premiere verwendet wird. Wichtig für das Verständnis ist, dass die Firma Beta Digital, welche auch zur Kirch-Gruppe gehört, für die Übertragungstechnik und damit auch für die Verschlüsselung von Premiere verantwortlich ist. Daher kommt auch der Name Betacrypt.

[9] http://de.wikipedia.org/wiki/Common-Scrambling-Algorithmus, 2005-01-25

[10] Premiere World Security Part 1, von C.Krätzer. M. Wenzel

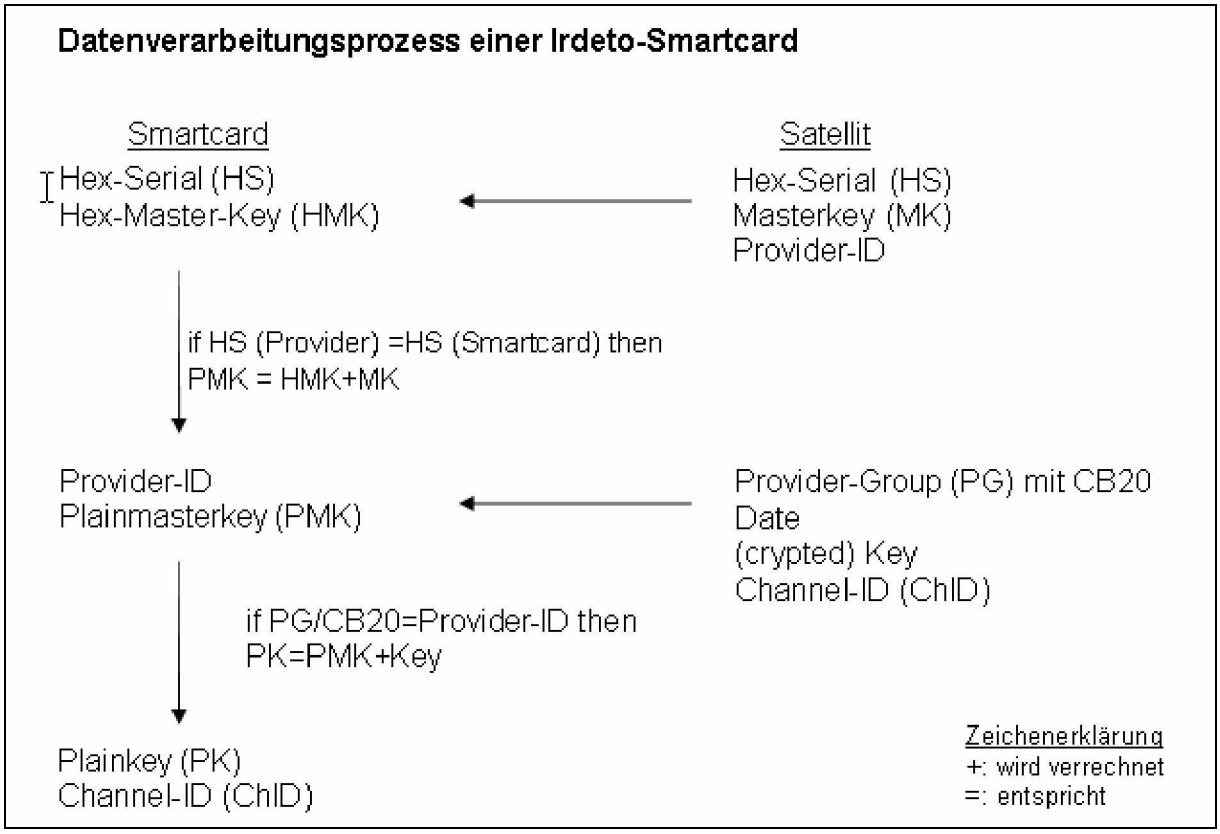

Abbildung 6: Key Austausch bei Irdeto

Da sich Irdeto und Betacrypt kaum von einander unterscheiden, beschreibe ich in diesem Kapitel hauptsächlich Irdeto. Der einzige markante Unterschied zwischen den Systemen besteht im so genannten Ländercode, welcher ein Merkmal einer Irdeto-Smartcard ist. Bei Betacrypt ist dieser GER für Premiere bzw. TEL (Telekom) für Mediavision. Beta Digital hat das Codierungssystem also sozusagen von Irdeto lizenziert und es mit gewissen Änderungen übernommen.
Eine Irdeto-Smartcard ist von außen nur durch den Schriftzug Irdeto und/oder der charakteristischen Seriennummer zu erkennen, welche meist seitlich auf der Karte aufgedruckt ist. Die Seriennummer ist auch in der Karte selbst abgespeichert. Nur ein Teil der Seriennummer, die so genannte Hex-Serial ist für den Dekodierprozess von Bedeutung. Die Hex-Serial ist 3 Bytes ($=2^{24}$ verschiedene Möglichkeiten) lang und genügt, um eine Karte eindeutig identifizieren zu können. Dies ist nötig, damit Karten vom Programmanbieter individuell angesprochen werden können. In allen Fernsehverschlüsselungsverfahren wird generell das Hexadezimalsystem verwendet. Im Innern der Karte unterscheidet man grundsätzlich zwei Einheiten: den Prozessor, der die Rechenoperationen durchführt und das EEPROM, das die Daten speichert. Der Prozessor hat zudem spezialisierte Krypto-Einheiten, welche RSA- und DES-Operationen sehr schnell durchführen können.
Der zweite Wert, der neben der Seriennummer (inkl. Hex-Serial) schon bei der Produktion auf die Karte geschrieben wird, ist der Hex-Master-Key (kurz HMK). Man könnte ihn als Hauptschlüssel zur Karte bezeichnen. Es ist (ohne Hacker-Techniken) nicht möglich, ihn von der Karte auszulesen. Er ist 10 Bytes lang, was einen großen Schlüsselraum zur Folge hat. Man unterscheidet nun grundsätzlich zwei Arten von Verschlüsselungscodes: die einen Codes, welche vom Programmanbieter über den Satelliten gesendet werden, und jene, die schon auf der Karte gespeichert sind.

Für die weitere Funktion der Karte sind nun erst einmal Codes vom Provider über den Satelliten nötig.
Die Smartcard enthält bisher nur eine Seriennummer, in welcher auch die Hex-Serial abgelegt ist und einen HMK. Diese Werte genügen aber noch nicht, um ein Fernsehprogramm dekodieren zu können. Zuerst muss die Karte noch vom Programmanbieter aktiviert werden. Dies geschieht über andere Verschlüsselungscodes, die über den Satelliten geschickt werden. Wird die Karte nun in den Decoder gesteckt, so erhält man nach einer gewissen Zeit den für diese Karte gültigen Masterkey (kurz MK, 8 Bytes), welcher nötig ist, um die Karte zu aktivieren. Zur Adressierung der verschiedenen Karten wird dabei die Hex-Serial verwendet. Pro Hex-Serial wird also grundsätzlich ein MK übertragen. Der Masterkey wird anschließend auf der Karte mit der HMK verrechnet. Daraus ergibt sich der Plainmasterkey (kurz PMK, 8 Bytes). Auch auf die Karte wandert dabei die so genannte Provider-ID (3 Bytes lang). Diese ermöglicht es dem Programmanbieter, für die nun folgenden Operationen die Karte gezielt anzusprechen. Die ersten zwei Bytes der Provider-ID werden auch Provider- Gruppe genannt.

```
Auswertung eines Irdeto EMM-Streams erzeugt von Master-LOG V3.83
=================================================================

 Pay-TV Provider:   Prem World Sat C-Cards
 PID:   1000

-----------------------------------------------------------------
  Bereich: Master-Keys  <12>

HEX-Sr PR Pro-ID MasterKey          Date
7EEBE8 10 21EBFE 00D723537F74FDCB1B 0772
7EEBEA 10 21EBFC 00CFDFA1245B69762E 0772
7EEBEC 10 21EBFA 001614DABC6DF5E81B 0772
7EEBF4 10 21EBF3 0029262F60166C3E1A 0772
7EEBF7 10 21EBF0 0047D328B7F1B8615E 0772
7EEBFB 10 21EBEC 001A3557B0ADF4C826 0772

7EEC06 10 21EBE1 00184749C2280AE56B 0772
7EEC08 10 21EBDF 00D259168D3171371D 0772
7EEC0B 10 21EBDC 005A57C214E822B697 0772
7EEC10 10 21EBD7 00C94824DB08863863 0772
7EEC11 10 21EBD6 0074AA10C82FDE9DC9 0772
7EEC12 10 21EBD5 0083B85CDA8B456702 0772
```

Abbildung 7: Beispiel: geloggte Master-Keys aus dem Satellitensignal bei der IRDETO Verschlüsselung[11]

Interessant ist hierbei, dass ein PMK nicht nur für eine Provider-ID sondern für eine ganze Provider-Gruppe gültig ist. Das entspricht immerhin 256 Karten (=1 Byte in Hex). Dieses ist eine der größten Schwächen des Irdeto-Systems. Da aber der Programmanbieter jede Karte einzeln ansprechen möchte, muss er auf das so genannte CB20-Nano zurückgreifen. Das CB20-Nano ist im Prinzip eine einfache binäre Maske, die die individuelle Adressierung ermöglicht.
Dieses ändert jedoch nichts daran, dass ein PMK für die gesamte Provider-Gruppe gültig ist. Die einzelnen Signale an die Karte werden mit dem CB20-Nano bloß unterdrückt.

[11] http://www.iswitch.ch/ma.pdf

Es gibt noch diverse andere Nanos, die hauptsächlich für die Kartenverwaltung verantwortlich sind. Sie spielen jedoch eher eine nebensächliche Rolle für die Dekodierung.

Nun sind auf der Karte also HMK, HS, PMK und Provider-ID gespeichert. Die zur konkreten Entschlüsselung des Fernsehprogramms benötigten Schlüssel befinden sich aber immer noch nicht auf der Karte. Dazu müssen erst noch (crypted) Keys vom Programmanbieter auf die Karte gelangen. Die Keys sind nur mit der Provider-Gruppe adressiert. Im Folgenden geloggten Datenstrom ist dies gut zu erkennen (2D58xx). Für xx lässt sich ein beliebiger Wert einsetzen.

Wenn man den nun empfangenen Key und sein Empfangsdatum (Date) mit dem PMK verrechnet so erhält man einen Plainkey (PK, 8 Bytes + 1 Byte für Keynummer). Pro Provider (also pro PMK) hat es für 18 PKs Platz. Meist werden aber nur die geraden Keynummern verwendet. (In unserem Fall handelt es sich um Key Nr. 08) Die Plainkeys sind die eigentlichen Dechiffrierschlüssel der Fernsehprogramme. Im Prinzip reicht es für einen Hacker aus, gültige Plainkeys auf seine Karte zu schreiben, um das Programm zu dekodieren. Dem wird aber mit Keyupdates entgegengewirkt. Die Plainkeys verfallen nach einer vom Programmanbieter bestimmten Zeit.

Auch im Datenstrom mitgeloggt wurde hier die zum Key passende Channel-ID (ChID, 2 Bytes). Die Channel-ID wird zwar nicht zur Decodierung benötigt, verwaltet aber die Berechtigungen der einzelnen Kanäle.

```
Auswertung eines Irdeto EMM-Streams erzeugt von Master-LOG V3.83
=================================================================
 Pay-TV Provider:   Prem World Sat C-Cards
 PID:   1000
-----------------------------------------------------------------
  Bereich: Keys der eigenen CardGroup  <1>

Pr CGroup Key                Date D-ID Type ChID
10 2D58xx 08=>083EDFF8CF9E7C52F1 0772 0771 1009 7D27

      à   Plainkey: B252018806244CFD (PMK:BEA7C566DC6C8AB2)
```

Abbildung 8: Irdeto EMM Stream [12]

Jetzt sind alle Daten auf der Karte vorhanden, um das gewünschte Fernsehprogramm dekodieren zu können.

5.2.1 Nano Codes

Nanos sind 2 Bytes lange Befehle die im EMM Datenstrom mit übertragen werden. Das 1. Byte steht für die Instruktion und das 2.Byte für die Länge des folgenden String.
z.B.:
– Datum
– Neue ProviderID
– Set Key (1. Byte ist die key-number, gefolgt von 8 Bytes des aktuellen key)
– Set Multikey – 2 keys im selben Kommando

[12] http://www.iswitch.ch/ma.pdf

- Set Multikey – 4 keys im selben Kommando
– Activate Channel ID (2 Byte chanID, 2 Byte Datumsstempel + 2 Byte Timer)
- CB (20) spricht mehrere Karten innerhalb einer Kartengruppe an.

5.3 Irdeto II

IRDETO-2 ist eine Weiterentwicklung von IRDETO. Der Unterschied zwischen Irdeto2 und dem Vorgänger besteht in der Verwendung eines so genannten CAM-Key, mittels dessen die Kommunikation zwischen CAM und der Smartcard verschlüsselt ist.

5.4 Viaccess

Dieses System wurde von France Telecom kreiert. Es findet Anwendung bei verschiedenen Fernsehstationen, unter anderem auch beim Schweizer Fernsehen. Technisch gesehen geht das Keymanagement ähnlich wie bei Mediaguard vonstatten. Viaccess unterscheidet sich von Mediaguard aber durch einen anderen und vor allem komplexeren Algorithmus. Viaccess muss der halbdigitalen Eurocrypt- Verschlüsselung ähneln, welche auch Smartcards verwendet. Steckt man nämlich eine Eurocrypt-Smartcard in ein Viaccess-CAM, so wird diese eigenartigerweise erkannt. Viaccess wurde erst anfangs 2001 geknackt. Mittlerweile existiert auch hier ein Nachfolgesystem namens Viaccess II.

5.5 Cryptoworks

(CAID 0D00h) Cryptoworks wird überwiegend auf Astra und Hotbird eingesetzt und beispielsweise von MTV2 genutzt. Auch der ORF bietet bereits seit April 2003 seinen Kunden die Möglichkeit, die ORF-Programme mit Cryptoworks zu entschlüsseln. Die alten BetaCrypt Smartcards werden noch bis Ende 2007 unterstützt.

5.6 SECA[13]

Es handelt sich hierbei um den Namen der Inhaberfirma (Société Européenne de Contrôle d'Accés) des Systems Mediaguard. Die Entschlüsslungsmodule werden von einer Firma namens Aston hergestellt.

Mediaguard ist eine französische Entwicklung. Das System wird hauptsächlich von Canal+ verwendet. Canal+ ist ein Programmanbieter, der in ganz Europa präsent ist.

Frankreich	CanalSatellite France
Italien	Tele + Digitale
Spanien	Canal Satélite Digital
Niederlande	Canal Digitaal Satelliet
Polen	Cyfra +

Der Mediaguard- Algorithmus funktioniert mittels einem 8 Byte langem encrypted ControlWord [CW] (über den Satelliten gesendet), mit dem anhand des Primary Key [PK] und Secondary Key [SK] (jeweils 8 Byte lang), ein auch 8 Byte langes plain (=entschlüsselt) ControlWord erzeugt werden kann. Dabei kann der Primary und der Secondary Keys derselbe sein. Der PK und SK werden auf der Smartcard mit 00 bis 0F indexiert, so dass insgesamt 16

[13] http://www.iswitch.ch/ma.pdf

verschiedene Keys verwendet werden können. Die Keys werden grundsätzlich in zwei Gruppen eingeteilt: die Management Keys [MK] (00 bis 0B) und die Operation Keys [OK] (0C bis 0E). Der Key 0F kann für andere Zwecke verwendet werden. Die MKs dienen dem Keymanagement, während die OKs für die eigentliche Decodierung des Fernsehprogramms zuständig sind.
Bei den erwähnten Keys handelt sich um so genannte Provider Keys, also solche, die stets nur einen Provider/Programmanbieter (vgl. Irdeto) betreffen. Es gibt jedoch auch SECA Keys, welche für das Providermanagement selbst notwendig sind. Diese sind aber nur bei der Kartenerstellung wichtig.
Der wichtigste Management Key ist der 01. Er ist vergleichbar mit dem PMK beim Irdeto-System. Das Pendant zur Irdeto Provider-ID ist die so genannte Programmable Provider User Address (PPUA, 4 Bytes). Die ersten drei Bytes der PPUA bilden die Shared Address [SA], das letzte, vierte Byte den Customer Word
Pointer [CUSTWP-Byte]. Die Shared Address ist mit der Provider-Group bei Irdeto vergleichbar.
Es lassen mittels einer SA nur Gruppen à 256 Karten ansprechen, während das CUSTWP-Byte die Adressierung einzelner Karten ermöglicht (vgl. Irdeto CB20- Nano). Mit dem MK01 und der passenden PPUA sind also Updates von OKs möglich.
Es fällt auf, dass das Mediaguard-System nur zweistufig arbeitet. Es gibt nur MKs und OKs. Bei Irdeto gibt es hingegen HMKs, PMKs und PKs. Dies ist für Hacker ein ziemlich großer Nachteil, denn PPUAs und MK01s haben den gleichen Geheimhaltungswert wie HMKs und Hex-Serials bei Irdeto. Der Grund liegt in der eindeutigen Identifizierbarkeit anhand der PPUA. Bei Mediaguard werden Karten meist individuell und nicht nur anhand der SA adressiert.
Weitere Management Keys sind beispielsweise der Key 00, welcher als Berechtigungsidentifikation bei PayPerView -Ausstrahlungen dienen kann, und der Key 02, welcher eine zeitliche Begrenzung der Karte (etwa bei Probeabonnenten) ermöglicht.

Man kann gewisse Parallelen zwischen Mediaguard und Irdeto erkennen, trotzdem unterscheiden sich die Systeme vor allem durch ihre internen Algorithmen. Informationen über diese zu bekommen ist leider eher schwer, doch wären sie für das genauere Verständnis der Codierungssysteme sehr interessant.

5.7 SECA II

(CAID 0070h) SECA-2 ist der Nachfolger von SECA und wird derzeit in Frankreich, Spanien und Italien verwendet. SECA-2 ging denselben Weg wie Irdeto zu Irdeto2 und etablierte einen CAM-Key in der Kommunikation zwischen Smartcard und CAM.

5.8 Nagravision digital[14]

Nagravision ist eine Entwicklung des Schweizer Unternehmens Kudelski. Das System prahlt regelrecht mit seinem komplexen Algorithmus. Dieser ist so lang, dass er auf einer Goldwaferkarte keinen Platz mehr findet. Wie der Name bereits vermuten lässt, ist Nagravision der digitale Nachfolger des analogen Nagravision/Syster-Verschlüsselungssystems. Trotz aller Bemühungen wurde dieses System im Verlaufe des Jahres 2002 geknackt. Bisher senden nur einige uninteressante Sender aus Polen und Spanien in Nagravision.

[14] http://www.isat.info/

Wichtig ist, dass bei den Systemen Conax und Nagravision verschiedene Sicherheitsstufen existieren. Bisher ließen sich nur Sender knacken, die eine niedrige Sicherheitsstufe einsetzen. Ein Sender kann auf Wunsch auf eine höhere Sicherheitsstufe wechseln. Die Tatsache, dass das digitale Teleclub-Paket im Kabelnetz auch in Nagravision verschlüsselt ist, aber noch nicht geknackt wurde, lässt auf eine interessante Zukunft für die Hacker hoffen.

(CAID 1800h) Nagravision wird seit Oktober 2003 in Deutschland vom Bezahlfernsehsender Premiere sowie vom Kabel Deutschland-Ableger DigiKabel eingesetzt, nachdem die Smartcards des alten Verschlüsselungssystems BetaCrypt unsicher geworden sind. Besonderheit bei dem von Premiere eingesetzten Nagravision ist die Tatsache, dass die eingesetzten Smartcards weiterhin die "Sprache" von IRDETO/BetaCrypt sprechen - der eigentliche Controlword-Algorithmus aber mit Nagravisionstechnik arbeitet. Dies wurde erforderlich, um auch alten Dbox Version 1-Besitzern den Zugriff zu ermöglichen.

6 Angriffe auf das Schlüsselmanagement System[15]

6.1 Modifizierte originale Smartcards

Modified Original Smart Cards (MOSC) sind veränderte, originale Smartcards eines PayTV Anbieters. 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 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.
Bei den ersten Generationen der Smartcard-Software wurden noch 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 wären jedoch 2^{40} ($= 2^{5*8} \approx 10^{12}$) 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 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 $5 * 2^8 = 1280$ Operationen immer noch um etwa den Faktor 860.000.000 niedriger als bei einem sicheren Verfahren.

[15] http://thoic.com/icard/frameger.html, http://www.iswitch.ch/ma.pdf

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.

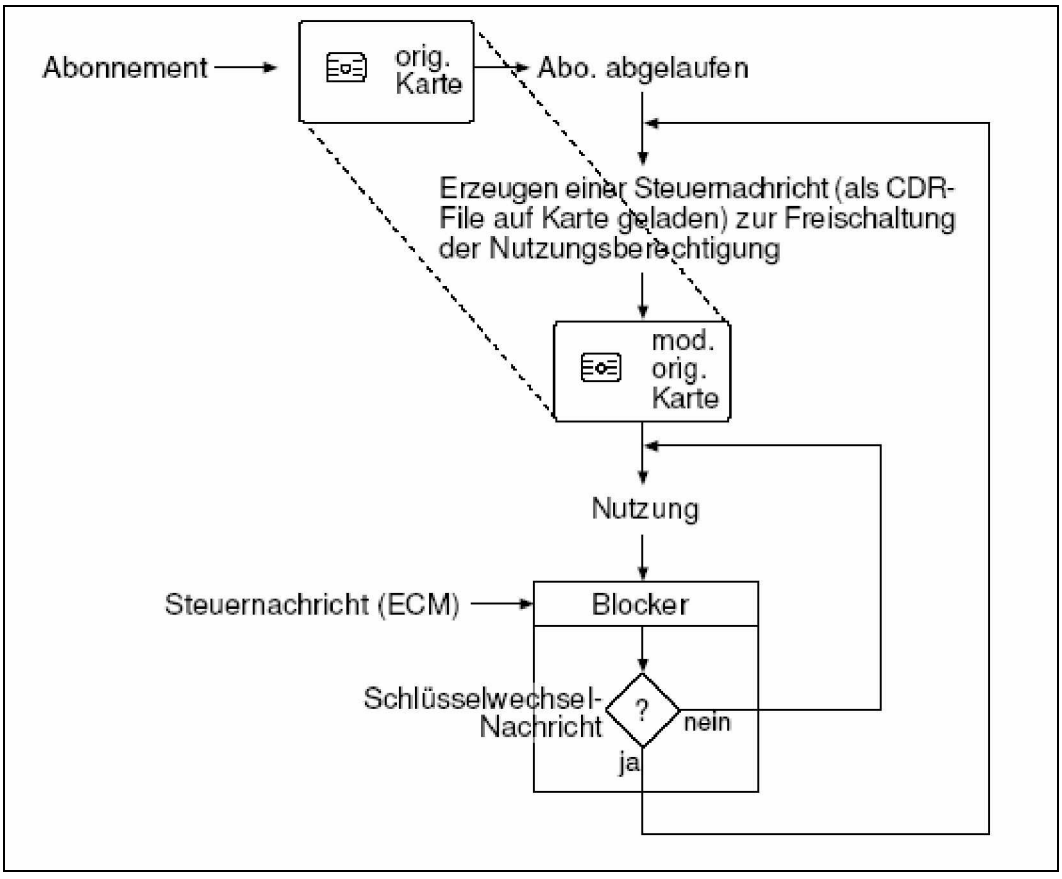

Abbildung 9: Angriffszyklus bei modifizierten originalen Smartcards

6.2 Chipkartenemulator

Bei der so genannten iCard kann die komplette Software auf der Karte erneuert werden. Bei häufigem Wechsel der Schlüssel wir einfach die Karte jedes Mal neu programmiert.

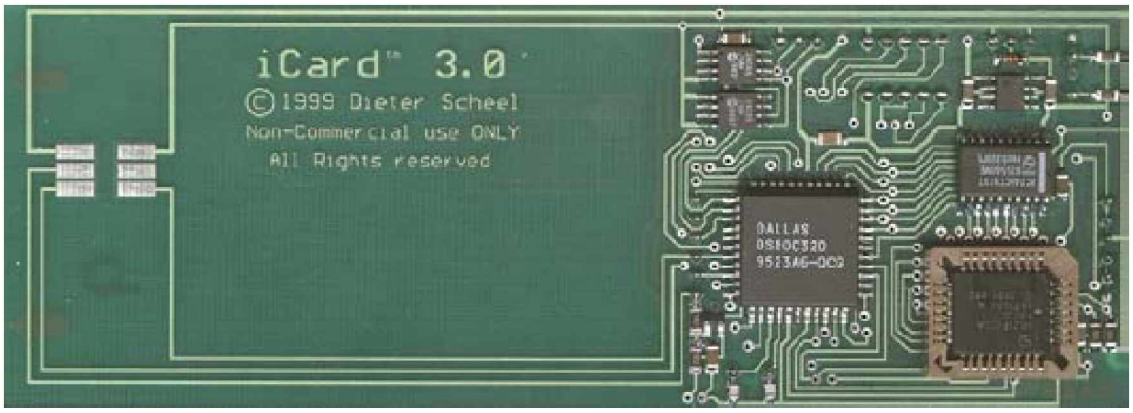

Abbildung 10: iCard

6.3 Season-Interface

Das Season Interface ist eine PC – Decoder Schnittstelle mit seriellem Kabel. Hierdurch wird die Simulation der Chipkarte durch einen PC durchgeführt (z.B. für VIACCESS, MediaGuard)
Das Interface benötigt nur noch die aktuellen kryptographischen Schlüssel. Diese gibt es im Internet in sog. Key-Datenbanken.

Abbildung 11: Season-Interface

7 Quellen und Literaturverzeichnis

http://www.tjaekel.de/dvb.htm, 2005-01-23

http://de.wikipedia.org/wiki/Common-Scrambling-Algorithmus, 2005-01-25

http://de.wikipedia.org/wiki/Conditional_Access_System, 2005-01-25

http://www.infomia.com/wiki,index,goto,Smartcard_System_für_DVB.html

http://www.moscwizzards.de.vu/ (Modifizieren von Smartcards)