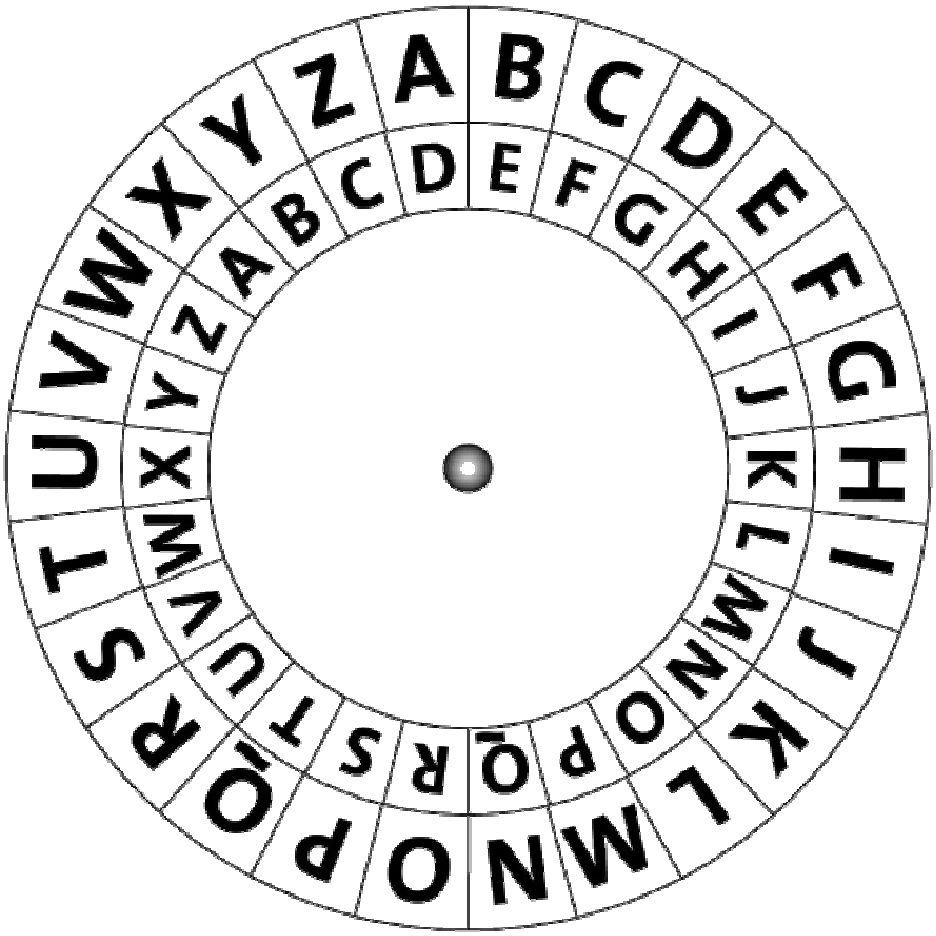
Verschlüsselungsverfahren für Medieninhalte

Am Beispiel Irdeto

Matthias Bach
FH Frankfurt am Main
Fachbereich 2 - Informatik



Inhaltsverzeichnis

Verschlüsselungen Anfang der 90er

Syster – Nagravison

Anfang der 90er Jahre gab es in Deutschland lediglich einen verschlüsselten TV Sender. Der Kanal nannte sich „TeleClub“ und wurde Ende der 90er durch den noch heute bekannten Sender „Premiere“ abgelöst. TeleClub sendet weiterhin in den Kabelnetzen der Schweiz. Anfangs wurde TeleClub und auch noch Premiere im recht einfachen Verschlüsselungsverfahren PayView3 codiert, welches als sehr einfach zu kompromittieren deklariert wurde. Entsprechend lag es nahe, die Codierung anzupassen, und ein weitaus sichereres System zu verwenden. So kam Mitte der 90er Jahre erstmals Syster-Nagravision als analoge Verschlüsselung der Firma Kudelski bei Premiere zum Einsatz. Syster-Nagravision wurde bis zur Abschaltung des analogen TV Programms von Premiere verwendet, und ist in Frankreich noch heute im Einsatz. Ein einziger TV Kanal (Canal+) sendet noch immer analog und in Syster verschlüsselt über Satellit. Syster basiert auf einer Vertauschung der Bildzeilen, die Vertauschung sieht zunächst völlig zufällig aus, basiert jedoch auf einem unbekannten Algorithmus, der ebenfalls nie bekannt wurde. Dennoch konnte Syster mit modernen Computern (Intel Pentium II. 400Mhz völlig ausreichend) kompromittiert werden, auf der Basis, dass die vertauschten Zeilen in Echtzeit zurückgetauscht werden, ohne das man den Vertauschungs-algorithmus kennt. Hierzu gehen wir zunächst etwas näher auf die prinzipielle Arbeitsweise von Syster ein, anhand eines Beispiels :

Abbildung 1

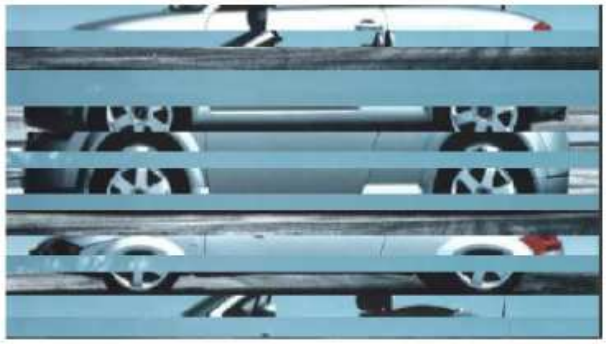


Abbildung 2

Wir nehmen ein Bild (Abbildung1) und zerschneiden es in 16 Blöcke. Diese Blöcke werden nun zufällig untereinander vertauscht (sog. Line Shuffeling). Es entsteht ein Bild, das als „verschlüsselt gilt“ und schlecht zu erkennen ist (Abbildung 2). Selbstverständlich ist der Person, die das Bild verschlüsselt hat, der Code bekannt, in welcher Reihenfolge das Bild wieder richtig zurückgesetzt wird. Nichts anderes wird durch den Decoder für PayTV Programme erzielt. Durch ausprobieren ist es nur schwer möglich, das Bild wieder korrekt zusammenzusetzen. Man bedenke, dass allein bei der Zerschneidung eines Standbildes in 16 Blöcke 32768 Permutationen möglich sind. Dieser Wert lässt sich sehr einfach berechnen, in dem man alle Möglichkeiten der Vertauschung abzüglich des korrekten Bildes berechnet.

$$2^{n-1} = 2^{16-1} = 2^{15} = 32768$$

Es liegt nahe, dass probieren eine zeitintensive Methode ist, ein Bild zusammenzusetzen. Nach dem Prinzip des Puzzles, man betrachte ähnlich farbige oder aussehende Teile und prüft, ob diese zusammenpassen, erreicht man wesentlich effizienter und schnell das Ziel, ein korrektes Bild zu erhalten.

Bei bewegten Bildern wird das gleiche Modell der Verschlüsselung angewendet, jedoch wird vielfach pro Sekunde ein Zeilentausch vorgenommen. Bei der deutschen TV Norm PAL haben wir 625 Zeilen für das TV Bild zur Verfügung. Es liegt also nahe, dass 625 Zeilen durch den Algorithmus ständig untereinander vertauscht werden. Visuell geht die Farbinformation für das menschliche Auge verloren, es entsteht ein grauer, zitternder Matsch, der das Ursprungsbild nur noch erahnen lässt. Das verschlüsselte Bild sieht wie in Abbildung 3 gezeigt, aus. Der Ton kann ebenfalls verschlüsselt werden, was jedoch separat durchgeführt werden muss, und nicht dem Algorithmus entspricht, der hier von Interesse ist.

Abbildung 3

Die Kompromittierung von Syster gestaltete sich für moderne Rechner relativ einfach. Man ging davon aus, dass ein TV Bild aus vielen Bildpunkten besteht (625 Zeilen x 576 Spalten). Jeder der 365760 Punkte leuchtet in einer bestimmten Farbe und Helligkeit. Analysiert man nun die Farbe und Helligkeit, und vergleicht Diese mit anderen Punkten, lassen sich schnell auf Zeilenebene benachbarte Zeilen finden. So ließ sich in Echtzeit sehr einfach wieder das komplette Bild durch Software zusammensetzen, mit dem Problem, dass bei Sendung, die viel gleiche Farb- und

Helligkeitsflächen hatten, nicht entschlüsselt werden konnten (grüner Rasen beim Fußballspiel, Abspann bim Spielfilm, da viel schwarzer Hintergrund).

Weitere Analoge Verschlüsselungen

Nebst Syster existierten viele weitere analoge Verschlüsselungsverfahren, jedoch ist heute keines mehr im Einsatz. In Europa am weitesten verbreitet waren Videocrypt I. (für Großbritannien) und Videocrypt II. (für Osteuropa), Eurocrypt in Verbindung mit der TV-Norm D2-MAC (für Skandinavien), Discret 12 (in Italien beim Staatsfernsehen RAI eingesetzt) sowie L-Crypt (in den Niederlanden verwendet und bereits 1995 durch die Digitalisierung der TV Übertragungen abgeschaltet). Weniger bekannt aber dennoch in Betrieb waren in den 90ern Smartcrypt, Nokia Line Shuffeling, Satpac und weitere, teilweise nur für EBU Übertragungen verwendete Verschlüsselungen. Videocrypt basierte ähnlich wie Syster auf einer Zeilenvertauschung, mit dem Unterschied, dass eine Zeile an einem Punkt zerschnitten und gekippt wird, und dann eine Vertauschung in der Zeile und Spalte stattfand. Auf einem ähnlichen Prinzip basierte auch Eurocrypt.

Abbildung 4

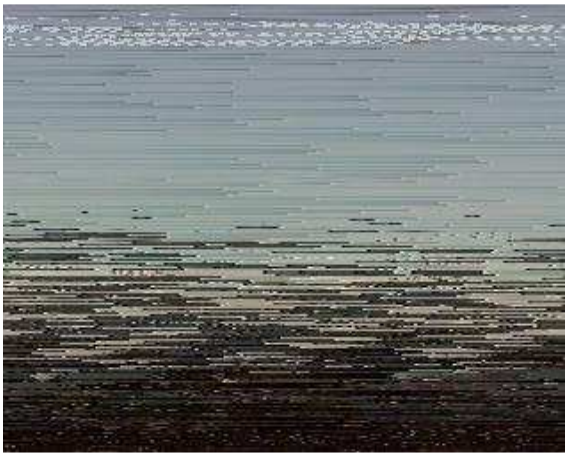


Abbildung 5

Die Abbildung 4 zeigt ein in Eurocrypt verschlüsseltes Bild, Abbildung 5 ist Videocrypt verschlüsselt. Bei beiden Systemen ist deutlich zu erkennen, dass sich hier das Ursprungsbild nichtmehr erahnen lässt, und Methoden zur Kompromittierung wie bei Syster keine Anwendung finden. Dennoch wurden beide Verschlüsselungen umgangen, nicht zuletzt, da sich zahlreiche attraktive Programminhalte dahinter verborgen fanden, die in ganz Europa großes Interesse fanden.

Mit der Umstellung Mitte der 90er Jahre auf die digitale Verbreitung von TV Programmen wurden auch digitale Verschlüsselungen entwickelt, und die analogen Codierungen verloren an Bedeutung.

Der DVB Standard

Für TV Veranstalter lagen die Vorteile von DVB klar auf der Hand. Günstigere Übertragungswege (auf einem Kanal, welcher analog nur ein Programm übertragen konnte, findet sich digital Platz für mindestens 7 Programme, je nach Kompression), bessere Bildqualität, Zukunftssicherheit, moderne & bessere Verschlüsselungen sowie eine weltweiter Standard (DVB-MPEG2) stellen nur einige Vorteile für Veranstalter dar. Daraus resultiert zwangsläufig eine Ausweitung von kleinen Spartenkanälen, Finanzeinsparungen und Benutzergruppenbezogenen Ausstrahlungen. Der DVB Standard (DVB = Digital Video Broadcasting) basiert auf der Übermittlung von Datenblöcken (Transport Stream / Container) mit 188 Bye Größe pro Container und einer Payload (Nutzlast bzw. Nutzdaten) von 184 Bytes.

Die ersten 4 Bytes stellen den Header des Containers dar, der sich aus einem Synchronisations Byte, einem Meldebit für Fehler, einer Paketkennzeichnung sowie der Transport Scrambling Control, die anzeigt, ob die Payload verschlüsselt oder unverschlüsselt (FTA = Free To Air) übertragen wird.

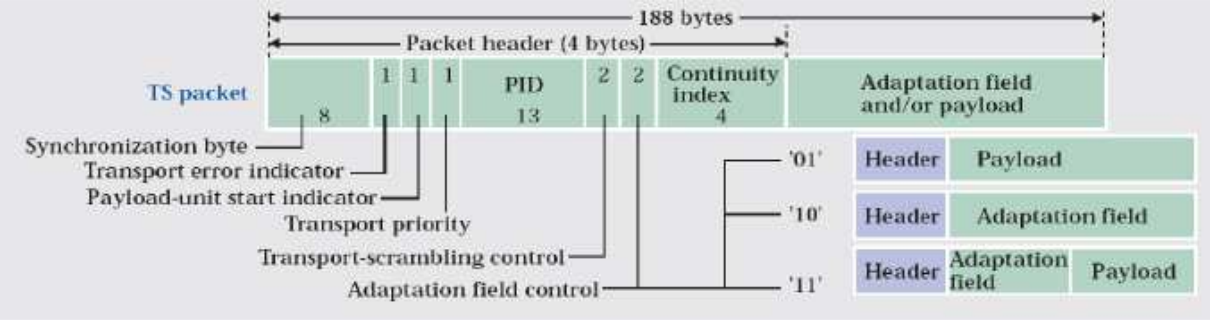


Abbildung 6

Weiterhin befinden sich im Header Bits für die Priorität des Containers und ein Payload Start Indikator. Dieser Aufbau (Abbildung 6) ist weltweit gleich, und wird weiterentwickelt, um Daten immer weiter zu komprimieren, speziell für Übertragungen im hochauflösenden HDTV Modus und um Kosten zu sparen. Aktuell kann über DVB auch in MPEG-4 übertragen werden (DVB-S2 Modus), dies findet bei HDTV Programmen und Zuführungen für Kabelkopfstationen Anwendung.

Mit dem Aufkommen von DVB wuchs auch die Anzahl verschlüsselter TV Programme, und somit die Attraktivität für Hacker, jene digitalen Signale zu kompromittieren. Allein Premiere besteht heute aus mehr als 50 Sendern, vor 10 Jahren noch war Premiere ein einziger, analoger TV Kanal. Somit ist eine sichere, harte Verschlüsselung der Programme notwendig, um das Überleben der TV Veranstalter zu sichern. Premiere, früher DF1, nutzte viele Jahre die Irdeto (BetaCrypt) Verschlüsselung, wechselte jedoch zwischenzeitlich auf Nagravision und neuerdings auf NDS Videoguard (notwendig, da die alten Systeme immer wieder gehackt wurden).

Die Verschlüsselung

Eine Verschlüsselung, wie Sie bei allen Anbietern zum Einsatz kommt, basiert auf dem Common Scramblig Algorithmus (CSA), der bei allen parallel existierenden Verfahren gleich ist. Die Verschlüsselung schützt demnach den CSA, sollte dieser bekannt werden, sind alle Verschlüsselungen unbrauchbar. Entsprechend gut gehütet ist dieser Algorithmus, jedoch lassen sich die Verfahren, den CSA zu schützen, durch Fehler und Lücken immer wieder kompromittieren. Während der Veranstalter dafür Sorge trägt, das System sicher zu halten, ist der Kunde durch eine Vielzahl von Kommunikationsprozessen im Verborgenen mit eingebunden, und erhält immer wieder alle Optimierungen und Verbesserungen online, die der Veranstalter dem Kunden übermittelt. Der Bedarf an Standards, die der Kunden vom Anbieter als Equipment erhält, ist entsprechend groß und wichtig. So wurde für die Kundenseite der Standard CAS (Conditional Access System) entwickelt, ein PCMCIA Modul mit Hardware, welche in der Lage ist, das Verschlüsselungssystem des Herausgebers des Moduls zu entschlüsseln, mit einer entsprechenden Smartcard des Anbieters, demnach ist das Modul mit Kartenleser für die Smartcard des Anbieters ausgestattet. Das CAM (Conditional Access Module) ist nebst PCMCIA Einschubgerät auch als Embedded Version in Receivern zu finden (Common Interface = CI), dadurch bieten sich für PayTV Veranstalter Synergien, dem Kunden gleich einen eigenen Receiver anzubieten, der kostengünstig ist und dem Kunden weitere Anschaffungen auf eigene Kosten erspart.

Abbildung 7

Das Ziel des Conditional Access Systems ist, ein 8 Byte langes Control Word (CW) zu generieren, welches die Payload im Container entschlüsselt und somit für den Kunden sichtbar macht. Das CW ist im o.g. Common Scrambling Algorithmus (CSA) verschlüsselt. Den Anfang macht die vom Anbieter herausgegebene Smartcard. Abbildung 7 zeigt Beispielhaft ein CAS Modul von Irdeto, rechts ist die Einbuchtung für den Einschub einer Smartcard zu erkennen.

Smartcards

Smartcards sind komplexe Mini Computer, die asynchron aufgebaut sind. Durch den asynchronen Aufbau wird erzielt, dass Zugriffe auf die Daten des Smartcardspeichers ausschließlich über den Mikroprozessor der Smartcard möglich sind. Dieses Feature stellt einen wichtigen Sicherheitsaspekt dar, um Speicherzugriffe von extern zu verhindern. Eine Smartcard besteht grundlegend aus zwei Einheiten, dem Mikroprozessor, und dem Speicher, einem EEPROM. Der Mikroprozessor enthält kryptographische RSA- und DES Einheiten (eingehende, chiffrierte Daten werden so entschlüsselt und im EEPROM abgelegt). Die Smartcard dient bei CA Systemen als Dekodierkarte für die in den Steuercodes enthaltenen Daten. Zu den Steuercodes folgen weitere Informationen auf der folgenden Seite.

Abbildung 8

Die Abbildung 8 zeigt eine NDS Videoguard sowie eine Nagravision Smartcard der Kabelnetzbetreiber KabelBW und ish in NRW. Mittels dieser Karten lassen sich je nach Buchung alle Sender im Kabelnetz des jeweiligen Anbieters öffnen.

Auf den Smartcards sind mehrere Informationen gespeichert. Im Auslieferungszustand sind lediglich eine Seriennummer (Hex Serial) und ein Hex Master Key (HMK) im EEPROM abgelegt. Erst durch die Inbetriebnahme im Conditional Access Module (CAM) werden in weiteren Schritten Daten auf dem EEPROM abgelegt, zum Beispiel ein signierter Plain Master Key (PMK) und eine Vielzahl an Service Keys (SK), üblicherweise 10 SK's auf einmal. Diese werden ebenfalls noch im Detail behandelt. Wichtig für den Betrieb einer Smartcard sind sog. Steuercodes, ohne die eine Smartcard nichts weiter als ein Mini Computer ohne Funktion bleibt.

Die Steuercodes

Steuercodes, ein elementarer Bestandteil einer komplexen Ver- und Entschlüsselungsstrategie, werden mit dem Datenstrom des Anbieters zum Kunden gesendet. Die Steuercodes gelangen Unidirektional über die regulären Verbreitungswege der Payload zum Kunden, im Folgenden als Empfänger bezeichnet. Als die üblichen Verbreitungswege sind Satellit, Kabelfernsehen oder DVB-T (in den Niederlanden oder z.B. UK wird flächendeckend PayTV via DVB-T angeboten) bekannt. Mittels den Steuercodes kann eine Smartcard z.B. aktiviert oder deaktiviert werden, es gelangen aber auch die zur Decodierung wichtigen Schlüssel per Steuercodes auf die Karte des Empfängers. Sollten Softwareupdates für CAMs oder andere Hardware verfügbar sein, können Updates mittels der Steuercodes in die beim Empfänger befindliche Hardware übertragen werden. Die Steuercodes werden in Entitlement Management Messages (EMM) und Entitlement Control Messages (ECM) unterschieden.

EMM

Die EMMs adressieren einzelne Decoder oder Decodergruppen. Somit kann ein Endgerät beim Empfänger direkt adressiert werden, oder eine ganze Gruppe von Geräten mit spiezieller Software etc. versorgt werden. Als Beispiel lässt sich ein Softwareupdate für die Receivergruppe xyz via Satellit, Kabel etc. verbreiten und einspielen, während alle anderen Reciever nicht auf das Update reagieren. Die EMMs aktivieren oder deaktivieren die Smartcards und tragen Sorge dafür, dass die aktuellsten Service Keys des Anbieters im EEPROM der Karte abgelegt werden. Die Service Keys werden in regelmässigen Zeitabständen gewechselt (in der Regel täglich), um Hackern nicht die Möglichkeit zu geben, bei kompromittierten Karten einen Dauerbetrieb zu gewährleisten, indem ohne Zahlung ein Programminhalt gesehen werden kann (sog. Schwarz-Sehen). Die EMMs sind somit elementar und der Löwenanteil der Steuercodes, die übertragen werden. Die Übertragung der EMMs erfolgt über logische Kanäle (PIDs). Dies logischen Kanäle sind fester Bestandteil jeder verschlüsselten Ausstrahlung. Um die PIDs zu organisieren (es ist nicht ur ein PID, sondern eine Vielzahl verschiedener PIDs), legt jeder Receiver beim Einschalten eine Conditional Access Table (CAT) an, um die EMM PIDs kennen und verwenden zu können. Der Aufbau der CAT wird ebenfalls übe reinen PID übertragen, den PID 0x01h. Ein EMM ist eine chiffrierte Nachricht, die mittels des PMK, der auf der Smartcard gespeichert ist, dechiffriert wird. Würde man EMMs in Klartext üertragen, wäre es problemlos möglich, die EMMs zu loggen, und anhand der geloggten Daten die Signale zur Kartenaktivierung und Deaktivierung herauszulesen.

Eine Aktivierung bereits Deaktivierter Karten wäre also möglich, was zu einem wirtschaftlichen Schaden des PayTV Veranstalters führen würde. Eine hohe Chiffirierung der EMMs ist als wichtig für ein sicheres Verschlüsselungssystem.

ECM

Die Entitlement Control Messages (ECMs) werden, wie auch schon die EMMs, in der CAT verwaltet, und per Satellit, Kabel, DVB-T usw. zum Empfänger übermittelt. Die ECMs enthalten das aktuell gültige CW für den CSA Descrambler, also die letzte Instanz, um ein verschlüsseltes Signal beim Empfänger sichtbar zu machen. Ebenfalls wird per ECM die Nummer des aktuellen Service Keys übertragen, mit dem das aktuelle Control Word entschlüsselt werden muss. Weitere Inhalte der ECM wären z.B. ein Zeitstempel (Timestamp), der notwendig ist zu Verrechnung mit weiteren Daten, abhängig vom verwendeten Verschlüsselungssystem. Im Beispiel Irdeto wird zu einem späteren Zeitpunkt auf diese Verrechnung eingegangen.

Common Scrambling Algorithmus

Das Herz einer Verschlüsselung stellt der CSA (Common Scrambling Algorithmus) dar. Dieser ist, wie bereits erwähnt, die eigentliche Verschlüsselung, und wird durch die Chiffriermethoden Irdeto, Seca, Nagravision etc. geschützt. Sollte der CSA bekannt werden, wären alle CAMs und CI Receiver unbrauchbar, und kein System mehr sicher. Absolut jeder verschlüsselte Programminhalt könnte decodiert werden, da der CSA Standard für jede DVB Konforme Übertragung ist, und daher nahezu Weltweit zum Einsatz kommt. Lediglich eine Hand voll Zuführungen, die über Satellit zu

Sendeanlagen übertragen werden und nicht für den Direktempfang geeignet sind, nutzen diesen Standard nicht. Diese Programm sind nicht DVB Konform und können auch nicht mit den üblichen Receivern empfangen werden. Diese Übertragung wird z.B. in Frankreich oder Spanien für Kabelanlagen verwendet, und erst in den Kopfstationen in DVB konforme Signale umgewandelt, um Zaungäste fernzuhalten.

Der CSA ist aus logischer Sicht nichts weiter als eine XOR Verknüpfung der zu verschlüsselnden Datenbytes mit einer Pseudozufallszahlenfolge. Die Pseudozufallszahlenfolge wird durch die Finite State Machine (FSM) erzeugt, das mehrfach angesprochene Control Word (CW) legt den Startzustand der FSM fest. Somit schließt sich der Kreis, dass das CW notwendig ist, um die Container zu entschlüsseln, die ja letztendlich in Ihrer Chiffrierung auf das CW zurückzuführen ist. Diese Art von Reverse Engineering nennt man klassisch „Entschlüsseln“. Somit wären die Schritte, wie Verschlüsselt und Entschlüsselt wird, im Grundaufbau klar. Nun folgt das was der Endkunde unter Verschlüsselungssystem mit den Namen Nagravision, Irdeto, Cryptoworks usw. kennt. Alle Systeme sind im Aufbau rund um den CSA gleich, erst was nach dem CW folgt, ist je nach System unterschiedlich. Alle Systeme haben das gleiche Ziel, ein CW zu generieren, um per Reverse Engineering den Datenstrom zu dechiffrieren.

Irdeto

Die ehemals in Deutschland und Österreich eingesetzte Verschlüsselung Irdeto ist wegen mehrfacher Kompromittierung inzwischen abgeschaltet worden, ist jedoch im Beispiel von Interesse, um den grundlegenden Aufbau eines Chiffriersystems zu erklären. Der deutsche PayTV Veranstalter Premiere setzte auf Irdeto bis zum Jahre 2006 (wenn auch getunnelt mit einem weiteren Chiffrierverfahren) und der ORF aus Österreich setzte bis 2008 auf das System. Aktuell wird Irdeto in einer weiterentwickelten Form noch in den Niederlanden, Griechenland etc. eingesetzt und gilt aktuell als sicher. Das CW bei Irdeto ist, wie allgemein bei nahezu alle Verschlüsselungsverfahren, 8 Byte lang und bietet somit eine 64 Bit Codierung, also 2^{64} Möglichkeiten, einen Schlüssel abzubilden. Würde man versuchen, das CW per Bruteforce Attacke zu erraten, und gibt man pro Versuch eine Zeit von 1µs an, würde die Attacke im Worst Case 500.000 Jahre dauern. Das CW gilt somit aktuell als sicher. Die Irdeto Smartcards sind allesamt mit einem Ländercode ausgestattet, der im EEPROM hinterlegt ist. Der Ländercode GER steht als Beispiel für Premiere, der Ländercode TEL für die „Deutsche Telekom“. Die Irdeto Smartcards sind im Auslieferungszustand lediglich mit der Seriennummer (Hex Serial) und dem Hex Master Key (HMK) ausgestattet, was bereits am Punkt „Smartcards“ erwähnt wurde. Der Hex Serial dient dazu, die Karte beim Empfänger initial zu Identifizieren, und mit weiteren Daten zu betanken. Der Hex Serial ist 3 Bytes, der Hey Master Key 10 Bytes lang.

Wenn diese „blanke“ Karte in den Receiver-Leseschacht oder das CAM eingelegt wird, erfolgen die folgenden Schritte, um die Karte zu aktivieren und zu benutzen. Alle nun notwendigen Daten werden über den Übertragungsweg (Sat, Kabel etc.) zur Karte gesendet.

- Die Karte erhält zuerst einen Masterkey (MK) der 8 Bytes lang ist, und die Smartcard aktiviert. Dieser Key ist ein Steuercode aus der Kategorie EMM.
- Der MK wird auf der Karte mit dem HMK durch den Mikroprozessor verrechnet, das Ergebnis ist 8 Byte lange Plain Master Key (PMK)
- Eine Provider-ID (Prov. ID) wird auf die Karte übertragen, 3 Bytes lang, Diese dient zur Identifizierung der Karte für weitere Operationen. Von den 3 Bytes der Prov.ID stellen 2 Bytes die Provider Gruppe dar. Ein generierter PMK gilt immer für eine ganze Provider-gruppe, nicht für einzelne Provider IDs. Dadurch sind lediglich 256 Karten adressierbar, in Umlauf sind je nach Anbieter mehrere Millionen Karten. Um dennoch Karten adressieren zu können, werden zur Abhilfe Binärmasken verwendet, im Falle der Providergruppe der CB20 Nano.
- Es befinden sich auf der Smartcard nun der Hex Serial (HS), der Hex Master Key (HMK), der Master Key (MK), der Plain Master Key (PMK) sowie die Provider ID
- Nun werden die eigentlichen Keys auf die Karte übertragen. Diese Service Keys werden anhand der Providergruppe Adressiert, können also an mittels CB20 Nano an einzelne Karten beim Kunden verteilt werden. Liegen die eigentlichen Service Keys vor (in der Regel bei Irdeto 10 Stück), können diese nun verwendet werden.
- Ein gültiger Service Key wird mit dem Timestamp und dem PMK verrechnet, das Ergebnis ist ein Plainkey (8 Bytes lang & 1 Byte für die Keynummer). Dieser Plain Key entschlüsselt das Control Word (CW), welches letztendlich der Startwert der FSM festlegt, und somit Grundbaustein beim entschlüsseln der Payload bzw. des Containers darstellt. Somit ist der Kreis der Entschlüsselung geschlossen.

Warum nun mehrere Service Keys (10 bei Irdeto, mehr sind möglich) auf der Smartcard abgelegt werden kann schnell verdeutlich werden. Würde man nur einen Service Key auf der Karte speichern, und mit dessen Hilfe das CW für die FSM dechiffrieren, würden alle Programme das PayTV Anbieters sichtbar werden. Der Anbieter hätte also keine Möglichkeit, verschiedene Pakete anzubieten oder PayPerView Dienste anzubieten. Für jedes Paket, jeden PPV Dienst etc. liegen eigene Service Keys bereit. Entsprechend hoch muss die Zahl der SK‘s sein, um diese Dienste abdecken zu können.

CB20 Nano

Diese Nano Code ist, wie bereits erwähnt, eine Binäre Maske, um das Defizit bei der Adressierung der Karten auszugleichen. Ohne den CB20 Nano wären lediglich 256 Karten Adressierbar. Nano Codes sind 2 Bytes lange Instruktionen, die im EMM Datenstrom mit übertragen werden, und als 1. Byte eine Instruktion sowie im 2. Byte die Länge des Folgestring halten. Ein Folgestring wäre z.B. das Datum, eine Provider ID, der Befehl Set Key oder ähnliches. Nebst dem CB20 Nano existieren auch weitere Nanos für Beispielsweise die Smartcardverwaltung.

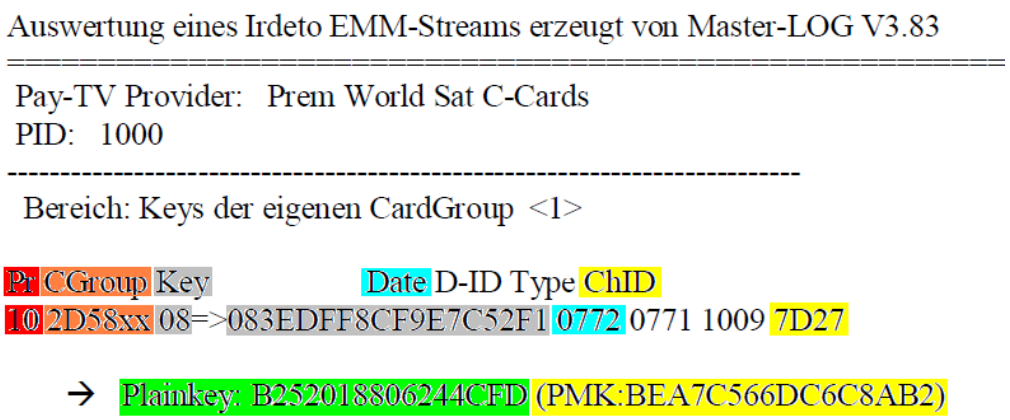
Logging von Master Keys bei Irdeto

Im nun folgenden Log sind die Master Keys der Irdeto Verschlüsselung erkennbar.

```
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
```

In gelb markiert sind die verschiedenen Hey Serials, die übertragen werden, um Smartcards anzusprechen. In Rot ist Nummer des Providers angegeben, gefolgt von der Provider ID, die auf der Smartcard abgelegt wird. In grün markiert ist der Masterkey erkennbar, der ja bekanntlich eine Smartcard aktiviert. Am Ende findet sich noch das aktuelle Datum des Datenstroms. Der gezeigte Log ist folglich ein Datenstrom, der diverse Smartcards aktiviert, die durch den Anbieter neu herausgegeben wurden oder Karten, die beim Kunden temporär deaktiviert wurden.

Logging eines EMM Streams bei Irdeto



Der nun gezeigte EMM Log mit der ID 2D58xx zeigt einen aktuell gültigen Plainkey in grün. Dieser Key wurde durch die Verrechnung des Service Keys 08 (in grau) mit dem Datum (hellblau) und dem Plain Master Key (in gelb) ermittelt. Ebenfalls mit angegeben ist die Channel ID, die für die Entschlüsselung nicht von Bedeutung ist. Die Channel ID ist, wie der Name schon sagt, die ID eines bestimmten TV Programms, welches letztendlich mittels Service Key 08 für den Kunden entschlüsselt wird.

Irdeto II.

Da Irdeto durch die Hacker zum Fall gebracht wurde, und die verschlüsselten Inhalte so für Jedermann zugänglich waren, musste das System weiter verbessert werden. Man entwickelte eine weitere Sicherheitsstufe, indem man die Kommunikation zwischen der Smartcard und dem CAM oder CI mittels eines CAM Key ebenfalls verschlüsselte. Dieses zutun einer weiteren Sicherheitsstufe war die Geburt des Irdeto Nachfolgers Irdeto II. Ansonsten wurden keine großen Änderungen am System vorgenommen außer das man die Smartcards ausgetauscht hat (neue Hardware war notwendig, da die alten Irdeto I. Karten einen Bug hatten, und sich mittels Buffer Overflow leicht kompromittieren ließen) und Software Updates beim Empfänger vornehmen musste.

Seca

In Konkurrenz zu Irdeto stehen ein Vielzahl an Verschlüsselungssystemen gegenüber. Als weiteres Beispiel für ein Chiffriersystem sollte an dieser Stelle Seca genannt werden, da Premiere ebenfalls Seca als Verschlüsselung nutzte. Seca wurde in Frankreich entwickelt und ist dort noch immer im Einsatz, ebenso in Polen, Spanien etc.

Seca basiert ebenfalls auf einem 8 Byte langen CW, welches aus einem Primary Key (PK) und einem Secondary Key (SK) errechnet wird. Die PKs und SKs werden in Management Keys (MK) und Operation Keys (OK) aufgeteilt. Der Management Key MK01 ist mit dem PMK bei Irdeto vergleichbar.

Eine Provider ID existiert bei Seca ebenfalls in leicht abgewandelter Form, Sie wird bei Seca jedoch Programmable Provider User Address (PPUA) genannt.

Da Seca ebenfalls kompromittiert wurde, ist gegenwärtig Seca II. sicher im Einsatz.

Weitere Informationen

Es besteht nach wie vor ein Koexistenz verschiedener Verschlüsselungsverfahren am Markt. So verwendet Beispielsweise Premiere aktuell das System NDS Videoguard (nach dem Scheitern von Nagravision), Arena setzt auf Cryptoworks, Kabel Deutschland auf Nagravision, Kabelkiosk auf Conax und im Ausland sind ebenfalls viele Verschlüsselungen im Einsatz.

In Nischen werden manche Programme in BISS verschlüsselt (FOX Deutschland, National Geographic Channel Deutschland, earth.TV etc.). BISS ist ein System ohne Karte, hier werden die Endgeräte direkt adressiert angesprochen und freigeschaltet. Diese Verschlüsselung wird nicht bei Endkunden eingesetzt, sondern verschlüsselt das Signal der Programme, wenn man Sie vom Veranstalter zum Paketvermittler schickt.

Abkürzungsverzeichnis

CAS	= Conditional Access System
CSA	= Common Scrambling Algorithmus
TS	= Transport Stream (Datenpaket)
CW	= Control Word
EMM	= Entitlement Management Message
ECM	= Entitlement Control Message
PMK	= Plain Master Key
SK	= Service Key
CAT	= Conditional Access Table
PK	= Plain Key
PID	= Logischer Übertragungskanal für EMM/ECM
Prov. ID	= Provider ID von Irdeto
HS	= Hex Seriennummer
HMK	= Hex Master Key
SK	= Secondary Key
MK	= Management Key
OK	= Operation Key
PPUA	= Programmable Provider User Address

Quellenangabe

Wikipedia (Grundbegriffe CAS, CSA, Irdeto, etc.)

Hochschule Bremen – Labor für Computertechnik 04/05

www.iswitch.ch/ma.pdf

www.cl.cam.ac.uk/~mgk25/nagra.pdf

www.tjaekel.de/dvb.htm

TU-Darmstadt – Fachbereich Informatik (für CSA)

www.isat.info

http://thoic.com