

Digitale Televisie

Piraterij in de ether

Auteur: Aram Verstegen
Datum: 29 Oktober 2008

Contents

Inleiding	3
Digital Video Broadcasting	3
Infrastructuur	4
Afscherming van betaalde uitzendingen	4
Common Scrambling Algorithm	4
Coderingen	5
Sleuteluitwisseling	5
Conditional Access Module	6
Smartcards	6
Piraterij in het wild	7
Conditional Access Modules	7
Smartcards	7
Card files	7
Card sharing	7
Ontvangers	8
Tegenmaatregelen	8
Conclusie	9
Verklarende woordenlijst	10
Bronnen	11

Inleiding

Eind 2006 is in Nederland het aanbod van analoge televisiediensten via de ether beëindigd. Dit bleek nodig om ruimte in het spectrum te maken voor het aanbieden van digitale televisiediensten via de ether. Nederlandse kabelaanbieders zijn in 2003 al begonnen met digitale uitzendingen.

Het belangrijkste voordeel van een digitaal systeem is dat het efficiënter gebruik maakt van de bandbreedte waardoor meer data over het medium kan worden verzonden. Dat betekent meer zenders, high definition uitzendingen en meta-informatie zoals een elektronische programmagids. En wellicht, voor de nieuwsgierige techneut, een mogelijkheid om de overstap nog aantrekkelijker te maken...

Alle Nederlandse aanbieders die de digitale televisiemarkt aanspreken, conformeren zich aan de Digital Video Broadcasting (DVB) standaarden. Hoewel de recente doorvoering van digitale televisiediensten ervoor gezorgd heeft dat het grote publiek in aanraking kwam met DVB technologie maakt apparatuur voor digitale schotelontvangst al sinds midden jaren negentig gebruik van de DVB-S standaard. Dit betekent dat piraten deze standaard inmiddels grondig hebben kunnen analyseren en gaten hebben geslagen in de beveiligingsmechanismen ervan.

Dit paper behandelt de beveiligingsmechanismen voor digitale video content in DVB, de mogelijkheden tot het omzeilen daarvan en de zwarte markt die is ontstaan om dit te faciliteren.

Digital Video Broadcasting

Specificaties voor digitale televisiediensten zijn vastgelegd in de Digital Video Broadcasting (DVB) standaarden. De DVB familie van standaarden beschrijft onder andere specificaties voor verbindingen over de ether (DVB-T), satelliet (DVB-S) en kabel (DVB-C), alsmede standaarden voor aanverwante systemen zoals teletext (DVB-TXT), ondertiteling (DVB-SUB) en televisie via internet (DVB-IPTV/DVB-NPI). Eigenlijk dekt de term DVB de lading niet meer, aangezien het gebruikt kan worden voor het uitzenden van allerlei soorten data. In de regel wordt het echter gebruikt voor het uitzenden van MPEG data streams.

Op dit moment geniet DVB de meest wijdverbreide adoptie door fabrikanten, wellicht omdat het, in tegenstelling tot concurrerende standaarden als ACTS en OpenCable, een meer flexibele familie van samenwerkende standaarden heeft geproduceerd.

Het European Telecommunications Standards Institute (ETSI) ratificeerde de DVB-S en DVB-C standaarden in 1994, en DVB-T in 1997. Deze standaarden zijn kort nadien in gebruik genomen door commerciële aanbieders (in respectievelijk 1994 en 1998).

De standaarden zijn ontwikkeld door het industrieconsortium DVB Project.

“The DVB Project is an industry-led consortium of over 280 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others in over 35 countries committed to designing open interoperable standards for the global delivery of digital media services.”¹

Infrastructuur

Afscherming van betaalde uitzendingen

Binnen digitale televisie zijn er verschillende soorten uitzendingen:

- ongecodeerde, ongescramblede gratis uitzendingen (free to air)
- gecodeerde, ongescramblede gratis uitzendingen (free to view)
- gecodeerde, gescramblede betaalde uitzendingen (pay tv)
- gecodeerde, gescramblede betaalde uitzendingen die buiten het standaardpakket vallen (pay per view)

Ongecodeerde uitzendingen zijn door iedere ontvanger te verwerken. Een codering wordt in de regel gebruikt om sleuteluitwisseling voor gescramblede content te faciliteren. Op commerciële zenders wordt de stream gescrambled, en wel met behulp van het Common Scrambling Algorithm.

Common Scrambling Algorithm

Het Common Scrambling Algorithm (CSA) is gespecificeerd door het ETSI en in 1994 door DVB Project geadopteerd als encryptiealgoritme voor data streams in DVB. Tot 2002 was de specificatie alleen beschikbaar na het tekenen van een non-disclosure agreement (NDA) van het ETSI. Deze NDA verbiedt de licentiehouders het algoritme in software te implementeren, om zo *reverse engineering* moeilijker te maken.

In 2002 werd een softwareimplementatie, FreeDec, vrijgegeven. Door het disassembleren van deze software werden, na jaren van speculatie, de op dat moment nog ontbrekende details duidelijk.

Het symmetrische algoritme bestaat uit een combinatie van een 64 bits bytewise block cipher en een stream cipher met een gezamenlijke sleutel, die cascaderend worden toegepast op de data. Er zijn inmiddels pogingen tot crypto-analyse ondernomen. [WW2004],² Het stream cipher is bevonden zwakheden te vertonen.

“We showed that the stream cipher is weak and can be efficiently broken. We also pointed out some properties of the block cipher which eventually could be used in a successful attack. However, since the block cipher uses 56 rounds we believe that such an attack would have to use sophisticated techniques. Cryptanalyzing both stream and block cipher at the same time seems to be a task too daunting to attempt. Finding special cases where plaintext and corresponding ciphertext can be obtained that is encrypted with only one of the ciphers

¹ http://www.dvb.org/about_dvb/

[WW2004] (1, 2) Ralf-Philipp Weinmann & Kai Wirt. Analysis of the DVB Common Scrambling Algorithm.

² <http://eprint.iacr.org/2004/289/>

³ http://en.wikipedia.org/wiki/Common_scrambling_algorithm

facilitates easier cryptanalysis. For the stream cipher these are packets with a residue. A sufficiently long adaption field on the other hand can lead to packets which are only protected by the block cipher.” [WW2004]

Vooralsnog is er geen aanval in het wild gezien, maar er wordt heftig gespeculeerd:

“While CSA algorithm uses 64-bit keys, in reality only 48 bits of key are unknown, since bytes 3 and 7 are used as checksum bytes, and may be easily recalculated. This fact allows practical space-time tradeoff attack where 32 bits are brute-forced, 16 bits are calculated with memory tables built from ciphertext, and 16 bits calculated as checksum with a running time of $O(2^{16})+O(2^{16})$, which can be less than a second if implemented in FPGA hardware or on scalable architecture like cell processor.”³

Het is niet de vraag of, maar wanneer er een praktische aanval op CSA komt. Als dat gebeurt zijn *alle* DVB systemen kraakbaar.

Coderingen

De DVB standaarden specificeren de scrambling van video streams in het Common Scrambling Algorithm (CSA) maar laat aanbieders zelf een coderingssysteem kiezen dat wordt gebruikt om de CSA sleutel over te dragen. De routines voor het decoderen van de sleutel zijn vastgelegd in een hardwaremodule die de Common Access Module heet.

Er zijn diverse partijen die een coderingssysteem op de markt hebben gebracht. Hier volgt een overzicht van Nederlandse DVB aanbieders en het door hen gebruikte systeem.⁴

Aanbieder	Type	Fabrikant CAM
KPN Digitenne	DVB-T	Conax
CanalDigitaal	DVB-S	Mediaguard
UPC digitale televisie	DVB-C	Nagravision
Overige aanbieders	DVB-C	Irdeto

Sleuteluitwisseling

De frequent wijzigende CSA sleutel (control word) voor het descramblen van de video stream wordt eveneens versleuteld en met de video stream (*in band*) meegestuurd in een zogenaamde Entitlement Control Message (ECM). Het control word wijzigt meerdere keren per minuut. Voor het ontcijferen van het control word uit de ECM is een zogenaamde Conditional Access Module (CAM) en een smartcard met de sleutel nodig.

Ook worden er Entitlement Management Messages (EMM) verzonden (*out of band*). De CAM vergelijkt deze met de informatie op de smartcard. Als informatie zoals zen-

⁴ <http://forum.trosradar.nl/viewtopic.php?t=48578>

derpakket en codering op de kaart overeen komen met de informatie uit de EMM mag de CAM het control word uit de ECM proberen te decoderen met de sleutel op de kaart.

Op deze manier worden EMMs gebruikt om nieuwe (groepen) kaarten te activeren en oude kaarten te blokkeren. Deze EMMs verversen veel minder vaak dan de ECMs, meestal maandelijks. Echter, enkele aanbieders verversen hun sleutels uit angst voor piraterij tot wel 5 keer per uur.⁵

Een zender kan het control word tegelijk in meerdere ECMs met bijbehorende EMMs meesturen om meerdere CAMs te bedienen. (Dit wordt simulcrypt genoemd.) Sommige zenders, zoals CNN op de HotBird transponder, ondersteunen wel 7 verschillende coderingssystemen tegelijk.

Conditional Access Module

De CAM is een door een derde partij ontwikkeld proprietair apparaat, meestal een special purpose PCMCIA type-II kaart, die vaak een ingebouwde smartcardlezer heeft en in samenwerking met een smartcard de versleutelde ECMs kan ontcijferen. De CAM verwerkt ook de Entitlement Management Messages (EMM) en verifieert de informatie op de smartcard hiertegen, voordat het de ECMs zal decoderen. Zo'n PCMCIA kaart past in een Common Interface (CI) op de ontvanger, maar er zijn ook ontvangers met een ingebouwde (embedded) CAM.

Smartcards

De smartcard bevat een CPU chip met programmatuur en een (E)EPROM met keys die de CAM nodig heeft om de ECM te kunnen ontcijferen. Door het gebruik van een EEPROM is het voor de smartcard mogelijk zichzelf te automatisch te updaten (AU) met een nieuwe sleutel (operational key). Uit informatie op de chip kan de volgende key berekend worden, zoals dat ook in de backoffice van de aanbieder gebeurt.

Deze opzet is gekozen omdat het analyseren van de programmatuur op de chips van een smartcard specialistische apparatuur zoals een electronenmicroscop vereist. De ROM zelf is makkelijk uit te lezen, maar de software die de keys updatet is geheim. Het is natuurlijk een vorm van *security through obscurity*, wat een gemotiveerde aanvaller met een ruim budget niet zal kunnen weerhouden.

Dat is dan ook niet gebeurd, want er zijn inmiddels filesets van kaartsoftware voor verschillende coderingen met werkende AU in omloop geweest.⁶

⁵ http://en.wikipedia.org/wiki/Conditional_Access

⁶ <http://www.duwgati.com/nl/page.php?page=kod-introductie>

Piraterij in het wild

De voorbeelden die hier genoemd worden komen uit DVB-S toepassingen, maar zouden in meer of mindere mate ook kunnen werken op andere DVB systemen.

Conditional Access Modules

Er zijn CAMs in omloop die meerdere coderingssystemen in één module huisvesten.⁷ Ook is het mogelijk om een zogenaamde soft CAM te gebruiken, dat wil zeggen software die een CAM emuleert. Deze producten zijn ontstaan door het *reverse engineeren* van officiële CAMs.⁸

Smartcards

Het is mogelijk een door de aanbieder middels een EMM uitgeschakelde kaart te voorzien van nieuwe keys. We spreken dan van een Modified Original Subscriber's Card (MOSC). Echter, zelfs zonder ooit abonnee geweest te zijn is het mogelijk betaalde televisie te ontvangen. Er zijn tegenwoordig tientallen verschillende typen smartcards verkrijgbaar, door hun grootte meestal geschikt voor meerdere coderingssystemen tegelijk.⁹ Ze verschillen eigenlijk alleen in gebruikte CPU en grootte van de ROM. De meest gebruikte kaarten zijn programmeerbaar en worden blanco verkocht, maar er is ook een markt voor kant-en-klare illegale kaarten (meestal voor pornozenders) die hoogstwaarschijnlijk massaal geproduceerd worden door criminele bendes.

Card files

De software van smartcards voor verschillende soorten coderingen zijn geanalyseerd en *ge-reverse engineered* door middel van *scanning*, het af luisteren van de communicatie tussen de CAM en de smartcard. Deze software wordt online uitgewisseld in de vorm van zogenaamde card files. Card files bestaan uit een programma en data (sleutels en meta-informatie) welke geprogrammeerd kunnen worden in een specifiek type smartcard.

Het is hiermee mogelijk geweest een officiële smartcard te emuleren, zelfs met AU functionaliteit.

Card sharing

Doordat er door aanbieders steeds strenger wordt opgetreden tegen piraterij gaat de beweging steeds verder de anonimiteit in. Een manier die nog steeds werkt, en voorlopig zal blijven werken zal werken is card sharing. Op privénetwerken kunnen officiële keys worden gedeeld, zodat meerdere personen elkaars zenders kunnen bekijken. Softwaretools

⁷ <http://www.ozzsat.com/cams/>

⁸ http://en.wikipedia.org/wiki/Conditional_Access

⁹ <http://www.duwgati.com/nl/page.php?page=crd-inleiding>

als GBOX, CCcam en NewCS zijn gemaakt om dit principe te automatiseren. Je moet dan wel speciale software op de ontvanger installeren.¹⁰

Ontvangers

De Dreambox is een PowerPC met DVB-S ontvanger, harde schijf en twee CI slots voor CAM modules, die een aangepaste versie van GNU/Linux draait en CAMs kan emuleren via softcam, PVR functionaliteit heeft, card sharing software clients kan draaien en door de softcam logging triviaal maakt. In principe is een PC met DVB kaart op dezelfde manier te gebruiken.¹¹

Tegenmaatregelen

Aanbieders zijn uitstekend op de hoogte van al deze piraterij. Ze voeren middels fake ECMs geregeld aanvallen op illegale kaarten uit, waardoor deze uitgeschakeld worden zonder dat originele kaarten er last van hebben.

Piraten kunnen zich hiertegen beschermen door middel van een blocker. Dat kan hardwarematig gebeuren, maar dan heeft de kaart geen AU functionaliteit meer. Een softwarematige blocker leeft in de CPU en simuleert een key in de ROM. Hierdoor kunnen schadelijke commandos worden opgevangen, en wordt de ROM van de smartcard tegen de aanval beschermd.¹²

¹⁰ <http://www.eurocardsharing.com/>

¹¹ <http://www.duckfiles.org/dreambox/index.htm>

¹² <http://www.duwgati.com/nl/page.php?page=kod-introductie>

Conclusie

Er is door inspanningen van de satelliet hacking community veel informatie over DVB naar buiten gekomen. Dit wekt de indruk dat een hack die het systeem compleet opent niet ver weg is. Het kat-en-muis-spel tussen aanbieders en piraten zal zich voortzetten, ook op het in Nederland relatief nieuwe medium DVB-T. Het is praktisch mogelijk om abonnementen te card sharen, dat wil zeggen: te delen over meerdere DVB ontvangers via internet.¹³

¹³ <http://www.eurocardsharing.com/dvb-t-dvb-c-dab/f270>

Verklarende woordenlijst

AU

Auto Update: een mechanisme waarmee officiële smartcards zichzelf automatisch van nieuwe keys voorzien.

CA

Conditional Access: het reguleren van de toegang tot content
Beveiligingsmechanisme in DVB (DVB-CA)

CAM

Conditional Access Module: special purpose PCMCIA module die:

- de toegang tot content beheert
- het ontcijferen van versleutelde control words faciliteert
- de smartcard kan updaten met nieuwe abonnementsinformatie en sleutels

CSA

Common Scrambling Algorithm: het door DVB gespecificeerde symmetrische encryptiealgoritme (DVB-CSA)

CW

Control Word: de frequent wijzigende 64 bit sleutel voor CSA die versleuteld wordt meegezonden in een ECM

DVB

Digital Video Broadcasting: een standaard voor het uitzenden van digitale video

ECM

Entitlement Control Message: een stuurcommando voor de smartcard dat het versleutelde control word bevat

EMM

Entitlement Management Message: informatie over de abonnees van de zender die door de CAM wordt vergeleken met de informatie op de kaart

FTA

Free To Air: ongecodeerde, gratis te bekijken uitzendingen

FTV

Free To View: gecodeerde, gratis te bekijken uitzendingen

PTV

Pay TV: gecodeerde, gescramblede uitzendingen van commerciële aanbieders

PPV

Pay Per View: gecodeerde, gescramblede diensten van commerciële aanbieders die buiten het reguliere aanbod vallen.

Bronnen

- <http://www.cdc.informatik.tu-darmstadt.de/mitarbeiter/wirt.html>
- http://www.dvb.org/about_dvb/
- <http://eprint.iacr.org/2004/289/>
- <http://www.duwgati.com/>
- http://en.wikipedia.org/wiki/Common_scrambling_algorithm
- http://en.wikipedia.org/wiki/Smart_card_piracy
- http://en.wikipedia.org/wiki/Digital_Video_Broadcasting
- http://en.wikipedia.org/wiki/Conditional_access
- http://en.wikipedia.org/wiki/Conditional_access_system
- http://www.birds-eye.net/definition/e/ecm-entitlement_control_message.shtml
- http://www.birds-eye.net/definition/e/emm-entitlement_management_message.shtml
- <http://www.ozssat.com/cams/>