Espen de Toonder

THE HACKER’S GUIDE TO

The Hacker’s Guide to Irdeto CableCrypt, Volume 2

1- Introduction

Welcome to the second release of *The Hacker's Guide to Irdeto CableCrypt*. Lots of things have changed in this book since the last release. Mostly because this time around we had the opportunity to put our teeth into the housekeeper source code of one of the older Irdeto analogue systems called *Delta*. The newer systems called CableCrypt and ComCrypt all find their origins in this old scrambling system.

With this release, this guide should also not be seen anymore as an exclusive guide to CableCrypt, but more as a guide which focuses on all Irdeto analogue scrambling systems. As far as we know these have been, in chronological order, *Delta*, *CableCrypt* and *ComCrypt*. Each system is an update that builds and improves upon the basic foundation that was laid with the Delta system. So maybe future releases of this book might see a change of the title.

The structure of the book has been changed with this release also. It is not just a simple update of release 1, but more a complete re-write. I have had to rearrange some of the chapters. Writing a book like this is harder than I thought. Not so much regarding what to put in it, because I've got loads of stuff in my head, but more how to arrange it in a way that makes it all readable. It's very hard to put down all those tons of information in a way that is understandable and not too confusing to the reader, all the more because everything is connected in some way and it's very easy to go too much in detail in some places where you shouldn't. I just hope most of you will find it comfortable to read.

If you're looking for a step-by-step guide on how to hack CableCrypt then you're in the wrong place. If you have a hobbyist interest in scrambling systems and always liked to know how they (the broadcaster) manage to do this and that, then you're in good company, because that's what we're interested in as well. This is by far the most in-depth look into analogue Irdeto scrambling systems that is publicly available and you can bet we're going to keep it that way.

The only problem I have with this release is that I didn't have the time to go into technical details as deep as I wanted to. This will hopefully be different with the next release where I won't tie myself down by setting a deadline.

Some people ask me when we're going to hack CableCrypt. Well, we're currently busy hacking our way at the housekeeper. If a hack surfaces it will be a housekeeper hack which uses official CableCrypt or ComCrypt decoders. The ASIC is just too complex and too little is known about it for someone to be able to build a 100% pirate decoder yet. So the way it is now, Canal+ and other users of the CableCrypt/ComCrypt systems have very little to worry about when such a hack is released.

In the mean time, sit back and enjoy the second release of this book. As ever I'd appreciate any feedback you'd have. Both positive or negative criticism is welcome. Ofcourse you're also welcome to chat about stuff you know or suspect about Irdeto analogue scrambling systems.

Espen.

2 - History of CableCrypt

It began in Africa… South Africa that is. A then local pay-tv broadcaster called *M-Net* started broadcasting in 1986 and Irdeto delivered the conditional access system which was called *Delta*. The Delta system was the foundation of all the other systems that would follow like CableCrypt and ComCrypt. In fact, these systems are consecutive upgrades of the Delta system.

Delta started out very basic with no tier system or pay per view support. The audio was mono although the subscriber could select between soundtrack A and B by using a button on the decoder. The housekeeper in these decoders was an Intel 8751 and the ASIC was named Delta 5.0.

Around 1993 CableCrypt was first put into use in the Netherlands and Belgium by FilmNet and in Italy by Tele+. CableCrypt was a major improvement over Delta with the addition of a tier system, stereo sound, pre-enabling option and a pending shutdown option. The housekeeper software was now also kept in a more secure Texas Instruments TMS370 microprocessor. The ASIC was upgraded to Delta 5.3. The ASIC naming scheme is a dead give-away that Delta and CableCrypt are related.

In 1997 the latest Irdeto analogue system was released: ComCrypt. These are now the decoders being supplied by Canal+, Tele+, FilmNet Greece and M-Net. ComCrypt is a further improvement on CableCrypt with the addition of pay per view capability. Also design improvements have made these decoders much cheaper to manufacture. The housekeeper is now a secure Dallas 5002FP and the ASIC is called Delta 5.4 and has even more functions integrated than the previous releases, allowing for a smaller board.

The ComCrypt system is special in that the housekeeper's memory is totally reprogrammable. So if the broadcaster would want to, the housekeeper software could be replaced with new software, possibly invalidating the current compatibility that exists between all the systems.

3- How Does It Work?

CableCrypt scrambles both the video and the audio of the TV signal. The video scrambling is very simple and totally insecure. This is mainly because the system was originally developed in the early 1980's and digitally scrambled video like the methods used in VideoCrypt and EuroCrypt were unaffordable back then.

The tuner inside your television needs so called synchronisation pulses to "grab" onto the video signal. There are two kinds of synchronisation signals in a TV signal and those are horizontal and vertical. What the CableCrypt encoder at the broadcasting station does is, first of all, to remove these sync pulses. This is what causes your TV to go bonkers when you try to tune it to a scrambled CableCrypt signal. It cannot lock the video signal so it rolls all over the screen.

The system is also capable of changing the video polarity. This sounds very complicated, but what it really means is that the video signal can be made to look "negative". All the black colours become white etc. CableCrypt can alter the polarity on a line, field or frame basis although it is currently only altered randomly every few seconds.

The audio is scrambled as well and this is what really keeps the system together, because this is much tougher to hack than the video scrambling. The audio is sampled at a frequency of 31.250 kHz so it becomes a stream of digital information. Before it is transmitted it is encrypted with an algorithm which is supposed to be secret. Then it is included in a 36-bit data burst before each video line, the place where all the horizontal sync pulses were supposed to be. There are 625 lines in a PAL signal and 25 frames per second. So that's 625 x 25 x 36 bits per second streaming into the decoder. All this needs to be decoded in real time by the decoder's audio decoding circuitry which recovers the original, unscrambled digital audio by applying its secret algorithm. This decoded digital audio is then sent to a D/A converter which turns the data into analogue signals.

Approximately every second the encoder at the broadcasting station generates a 56-bit control word that is needed by the audio decryption circuitry to be able to decode the audio. You can see the control word as some kind of key which is needed. Ofcourse this control word is scrambled before it is transmitted and it needs to be decoded by a seperate chip before it can be used. Only authorised decoders will be able to decode the control word.

The encrypted control word is transmitted along with other data, like commands to individual decoders, in the first few invisible lines of the video signal which are also called the VBI (Vertical Blanking Interval). 50 times per second, 4 packets will be modulated into the VBI. The first one is always the encrypted control word or instructions to the decoder which involve the decryption of the control word, like when to give it to the audio decryption component, when the TV signal should be negative (video polarity) etc. The remaining 3 packets are always command packets and they contain decoder serial numbers and commands to these decoders. This way the broadcaster is able to control every single decoder by switching it on or off or more complex things like downloading a new decryption key to the decoder or tuning the decoder to the correct frequency for you automatically.

There are 2 chips inside a CableCrypt decoder which are referred to as the housekeeper and the ASIC. A housekeeper is, like the name suggests, the one which is more or less running the show in the decoder. It is equipped with the secret algorithm that decodes the control word and processes all the packets mentioned above. It is this chip that hackers will go after first.

The other one, the ASIC, is the one doing most of the hard work. First of all let me explain what an ASIC is for those who don't know. It stands for Application Specific Integrated Circuit and that just about sums up what it means. It is an IC which was *specifically* designed for a particular application. The Irdeto decoder in our example.

The client, Irdeto in this case, specifies to the chip manufacturer what the chip should do. Ofcourse this means you cannot simply buy an ASIC off the shelve or order one from your local electronics store.

The ASIC is the one that reconstructs the video signal by inserting sync pulses. It also demodulates the broadcaster's data packets from the VBI and the encrypted digital audio stream. It also houses the actual audio decryption algorithm. Do not confuse this with the control word decryption algorithm in the housekeeper. The ASIC is not able to decode the audio all by itself. The ASIC's algorithm needs the decrypted control word which changes each second. This is done by the housekeeper. So there's a constant stream of 2-way traffic between the housekeeper and ASIC. The ASIC sends 50 x 4 packets per second to the housekeeper which also contain the scrambled control word and the housekeeper returns the decrypted control word to the ASIC every second or so.

There are 2 other compatible systems out there besides CableCrypt which are called *Delta* and *ComCrypt*. Both are also Irdeto analogue systems and all the information in this chapter applies to these pay-tv systems as well. Delta was the forerunner to CableCrypt and ComCrypt is its successor.

4 – The Irdeto Control Word Algorithm

There are 2 important algorithms inside a CableCrypt decoder. The first one is inside the ASIC and is used to decrypt the digital audio stream and the second is the one inside the housekeeper which decrypts the scrambled control word, which is needed by the ASIC as input to its algorithm.

Little is known about the audio decryption algorithm inside the ASIC, but it's highly likely that it is a form of CBC, which stands for Cipher Block Chaining and really comes down to the audio data being hacked into 4 packets which are scrambled in succession and then transmitted. Each block uses the output of the previous block as input, excpet for the first block which uses a fixed value called an initialisation vector.

Irdeto applied for a patent that describes a reversed CBC algorithm which is more suitable in the case of conditional access systems where you have one or a small number of broadcasters (the encoder at the broadcasting station) and a multitude of receivers (the decoder at the subscriber's home) and it prevents hacking attempts which are based on trying to find a pattern because of the use of an initialisation vector.

In this document we're going to be focusing on the second algorithm which decrypts the control word and is present inside the housekeeper. You only need to hack the housekeeper to have a working hack. If you want a true 100% pirate decoder you will need to hack the ASIC as well, but that is perhaps a future mission. Anyway, for those interested in the mentioned patent, you can download it from the Republic's web site where you probably got this document as well.

Everything which is now described about the control word decryption algorithm is based on a ROM dump from an Irdeto Delta 9000 decoder. You won't find a complete description of the algorithm yet, because we want to save that for when we have managed to develop a custom housekeeper.

The algorithm in question is not only used to decrypt the control word, but for other purposes which I'll describe in the future. The algorithm works with 2 blocks of data which are, in case of control word decryption, both 8 bytes wide. One block contains the scrambled control word itself which the housekeeper has just received from the ASIC and the other block contains the decryption key which will be used to decode it. I'll get to the subject of decryption keys in a moment. The result of the algorithm can be found in the same block where the encrypted control word was.

What basicly happens is that the main function of the algorithm is called an `x` number of times, where `x` is 64 if we're dealing with control word decryption. Each round basicly does the following (we start with `i=0` and `j=0`):

```
Offset = Key[i] ^ Cword[j];
i++;
j++;
Cword[j] = Keytable[Offset] ^ Cword[j];
```

So what happens is that in each round a byte of the decryption key is XORed with a byte from the encrypted control word. This value is then used to create an offset into a 128-byte key table. The 7-bit key value which is picked up from this table is then used to XOR the next control word byte. The above code is very basic, because there is also ofcourse code which makes sure that pointers `i` and `j` are always pointing within the 8-byte block.

There is another added complexity which is perhaps used as an extra element to destroy any pattern forming. Every 9 rounds, the pointer `i` is not incremented while `j` is. Also the first XOR element is not performed in that case.

5 – Decryption Keys and Operational Keys

There are 2 types of keys used in the Irdeto analogue systems. The most important key is the decryption key. This is a 56-bit value that is used primarily by the Irdeto Control Word algorithm to decode the control word. The broadcaster has the ability to download a new decryption key to the decoder if that is necessary using an instruction that has been reserved for this purpose.

Under normal circumstances the decryption key which is stored in the EEPROM is used, but the broadcaster can also decide to use a fixed decryption key which is stored in ROM. This fixed decryption key is not changeable and is actually created by combining 8 consecutive values from the 128-byte key table inside the decoder's ROM. Why this possibility exists is not clear yet, because it is ofcourse a weakness to use a key that is unchangeable and known. My guess is that this fixed key is used when the broadcaster is downloading a new decryption key to the decoders. During this period the system is in a transitional stage and both the old and new decryption keys are in the field. The fixed key is then used for control word decryption until all the decoders have received the new decryption key and then the system switches to the new decryption key.

Besides the decryption keys we also have what I call operational keys. An operational key is only 7 bits wide and there are 16 of them in the system. They are used for several purposes which I haven't all investigated yet, but one of their most important functions is that they are used to create yet another key: the packet decryption key.

Some of the data packets are scrambled. You'll remember there are 4 packets received every 1/50th of a second. The first packet is either the control word packet which contains the scrambled control word or it is a control packet. The last 3 are always command packets which contain serial numbers and decoder commands. Well, the control packet is always scrambled and needs to be decoded by XORing it with the packet decryption key. Command packets are not always scrambled. The first 3 bytes are never scrambled because they contain a serial number. The remaining 5 bytes *can* be scrambled, but are not always that.

Just like the decryption key, the operational keys can be downloaded to the decoder by the broadcaster. This usually happens with 2 or more keys at a time.

6 – The Serial Number

Each decoder has a unique serial number. Compare it to an address so that the broadcaster is able to individually control a decoder by sending a command to your decoder's specific address.

The serial number is 22 bits wide with a 10 bit checksum. This means the system's subscriber limit is about 4 million. More subscribers cannot be carried, because the system cannot have more unique serial numbers. I'm not sure how the serial number can be translated from this value to the 9-digit value on the back of the decoder yet.

If the broadcaster switches your decoder on over-the-air after you call them it means your decoder has just received a command packet which was addressed to it. This command packet will start with the serial number of your decoder, followed by the command number which is used to identify a switch on command. Only your decoder will listen to this command ofcourse, just as it will ignore all other command packets which do not have its serial number in them.

It appears that there is also a serial number that all decoders will listen to and that is `00 0F 3F` and some variations on that. I haven't yet investigated in which conditions these serial numbers are used, but it is obvious that they can be used if the broadcaster wants to address all decoders in the field with one command packet. The broadcaster could e.g. download a new decryption key or operational key to all subscribers with one command.

7 – System Features

As is explained in chapter 2, which handles the history of the Irdeto Analogue systems, the system really began with Irdeto Delta. CableCrypt was released later and was a big improvement and only recently has ComCrypt been released which is the latest upgrade of the system. It is quite easy to spot the heritage of these systems because the ASIC is still called Delta 5.x. Where in the first Delta decoders this was 5.0 it has now been upgraded to version 5.4 in the ComCrypt decoders.

But there is a certain backward compatibility in all the new system which allows for all decoders to operate on the same signal. Right now in most countries both CableCrypt and ComCrypt decoders are used to decode cable versions of popular pay-tv channels like Canal+, Tele+ and FilmNet Greece.

The very first decoders, which were probably Delta 9000, were very basic. The system feature list of the original Delta system is much less impressive than that of the CableCrypt and ComCrypt systems. What follows is a list of the key features which were or were not present in the Delta, CableCrypt and ComCrypt decoders. Then a summary is made with explanation of the various features available.

Irdeto Delta 9000

Housekeeper:	Intel 8751 initially, later versions replaced by TMS370.
ASIC:	Delta 5.0, 5.1 and 5.2
EEPROM:	External 93C46 with the 8751, later onboard with the TMS370
Preset memory:	8 channels
Tier system:	No
Pay Per View:	No
Audio:	Mono, 2 soundtracks
Pre-enabling option:	No
Pending disconnect:	No
Parental control:	No
Remote tuning:	No

Irdeto CableCrypt 1

Housekeeper:	Texas Instruments TMS370
ASIC:	Delta 5.3
EEPROM:	Internal (housekeeper)
Preset memory:	39 channels
Tier system:	Yes (presumably 48 channels)
Pay Per View:	Possibly
Audio:	Stereo
Pre-enabling option:	Yes
Pending disconnect:	Yes
Parental control:	Yes, 6 levels
Remote tuning:	Yes

Irdeto ComCrypt 4000

Housekeeper:	Dallas 5002FP
ASIC:	Delta 5.4
EEPROM:	Internal (housekeeper)
Preset memory:	99 channels
Tier system:	Yes (48 channels)
Pay Per View:	Yes, room for 28 simultaneous PPV events
Audio:	Stereo
Pre-enabling option:	Yes
Pending disconnect:	Yes
Parental control:	Yes, 6 levels
Remote tuning:	Yes

Tiers

This defines how many different channels or groups of channels the system can carry. With so many channels out there it is required that the broadcaster can decide which channels the decoder can and cannot decode.

In the Delta system there was no way for the decoder to differentiate between multiple channels or tiers. It was only made for one pay-tv channel, which was M-Net at the time. The CableCrypt system introduced a tiering system which does allow use of multiple channels. The exact number of channels is unknown, but is presumably 48 which is the same as in the ComCrypt system.

Pay Per View

It is certain that the ComCrypt system supports Pay Per View. It has room for 28 events. The Delta system ofcourse didn’t have PPV at all. CableCrypt remains a bit of a mystery. It is possible that the system can do PPV, but at this point there’s no certainty about it. As far as I know PPV has never been used by any of the broadcasters yet. It will be interesting to see what Canal+ will do with their PPV plans in the future.

Pre-enabling option

CableCrypt and ComCrypt have a pre-enabling option, which is a special state the decoder is in when it is at a pay-tv dealer. It is a used featured by Canal+ in the Netherlands. What it means is that the decoder is already authorised to decode Canal+ as soon as it is taken out of the box. The idea is to allow people to sign up for the service and let them take the decoder home and watch straight away without waiting for authorisation over-the-air.

Pending disconnect option

If a subscriber is late with their payment or if there’s any other valid reason justifying shutdown of the decoder, the system is able to warn the subscriber that a shutdown is pending by using the front display. The numbers 93, 92 or 91 will be flashing meaning the decoder will be shut down in 3, 2 or 1 days. E9 will flash if the shutdown has been completed. The subscriber has this 3-day time period to contact Canal+ and clear up any errors which might have occured with their subscription payment.

Remote tuning of stored programs

The broadcaster can remotely tune every decoder to the correct frequency of its channel on a specific cable net. Because the Canal+ channels are available on different frequencies on various cable nets, not every decoder will have the same frequencies stored. Although it is custom that the decoders come preprogrammed with all cable channels available in the area where you sign up for a Canal+ subscription, this is not always the case and it is possible for a subscriber to move to a different cable area which uses different frequencies.

Ofcourse it is possible to manually tune program presets, but in some cases it is convenient for the broadcaster to be able to tune in the correct frequencies of e.g. Canal+ 1 and 2 into programs 1 and 2 of a subscriber’s decoder if they request so.

8 - Data Packet Structure

There’s a constant stream of data packets from the ASIC to the housekeeper. The housekeeper receives roughly 32 bytes per field, which means there are 50 of them per second. Each 32 bytes message can be split into 4 packets. The last 3 packets are always command packets. These contains serial numbers of decoders and commands to those decoders.

The first packet can be 2 things. It is either the encrypted control word or it is a control packet. The housekeeper can easily differentiate between the two by checking the start bit.

Control Word Packet
This is the scrambled control word that needs to be decoded by the housekeeper using its secret algorithm and the decryption key. A control word packet always has 7-bit bytes. The control word is 8 bytes plus a checksum byte so that means 63 bits are received.

Control Packet
This packet is standard 8-bit material. There are 8 bytes. This packet is scrambled and must first be descrambled by XORing it with the Packet Decryption Key. The first byte’s low nibble tells what should be done. Several things are possible. The high nibble of the first byte and the second, third and fourth byte can be compared to Operational Keys. The fifth byte is used to compare Operatonal Keys as well but in a different fashion. The exact meaning is not known yet, but under certain circumstances this comparison can lead to the decoder not decoding anymore.

The sixth byte is used to indicate the polarity of the video signal. Corresponding to the value in this byte the housekeeper will send a signal to the ASIC whether to invert the video signal or not.

Of the seventh byte only the lowest 2 bits are used. If bit 0 is set the housekeeper will return the decoded control word to the ASIC. This way the broadcaster is able to define when a new control word period starts. Bit 1, if it is set, will force the decoder to use the earlier discussed fixed ROM Decryption Key instead of the normal Decryption Key.

The eighth byte is a checksum.

Command Packet
A command packet is also 8 bytes in size. It contains a serial number, a command code and parameters which can be used by the command. The serial number is only 22 bits in size and it can be found unencrypted in the the first two bytes and the lower 6 bits of the third byte.

Bit 6 of the third byte is used to indicate whether the rest of the packet is scrambled. If it is set, the last 6 bytes of the packet are XORed with the Packet Decryption Key. Bit 7 is used to construct the command code together with the fourth byte. If the command has any parameters, then they are usually stored in the fifth, sixth and seventh byte. The eighth byte is a checksum.

If a decoder receives a command packet it will first check the serial number. If this does not match nothing happens. If it does match, the command code will be calculated and the command will be executed. There is room for 32 commands in Irdeto Analogue systems and not all of them were used in the Delta system. Ofcourse CableCrypt and ComCrypt will have more command codes to support their additional functions.

A command can do several things like switch off a decoder, download a new Decryption Key etc. In a future version of this doc I'll have a complete list of the available commands used in Delta decoders and what they do.