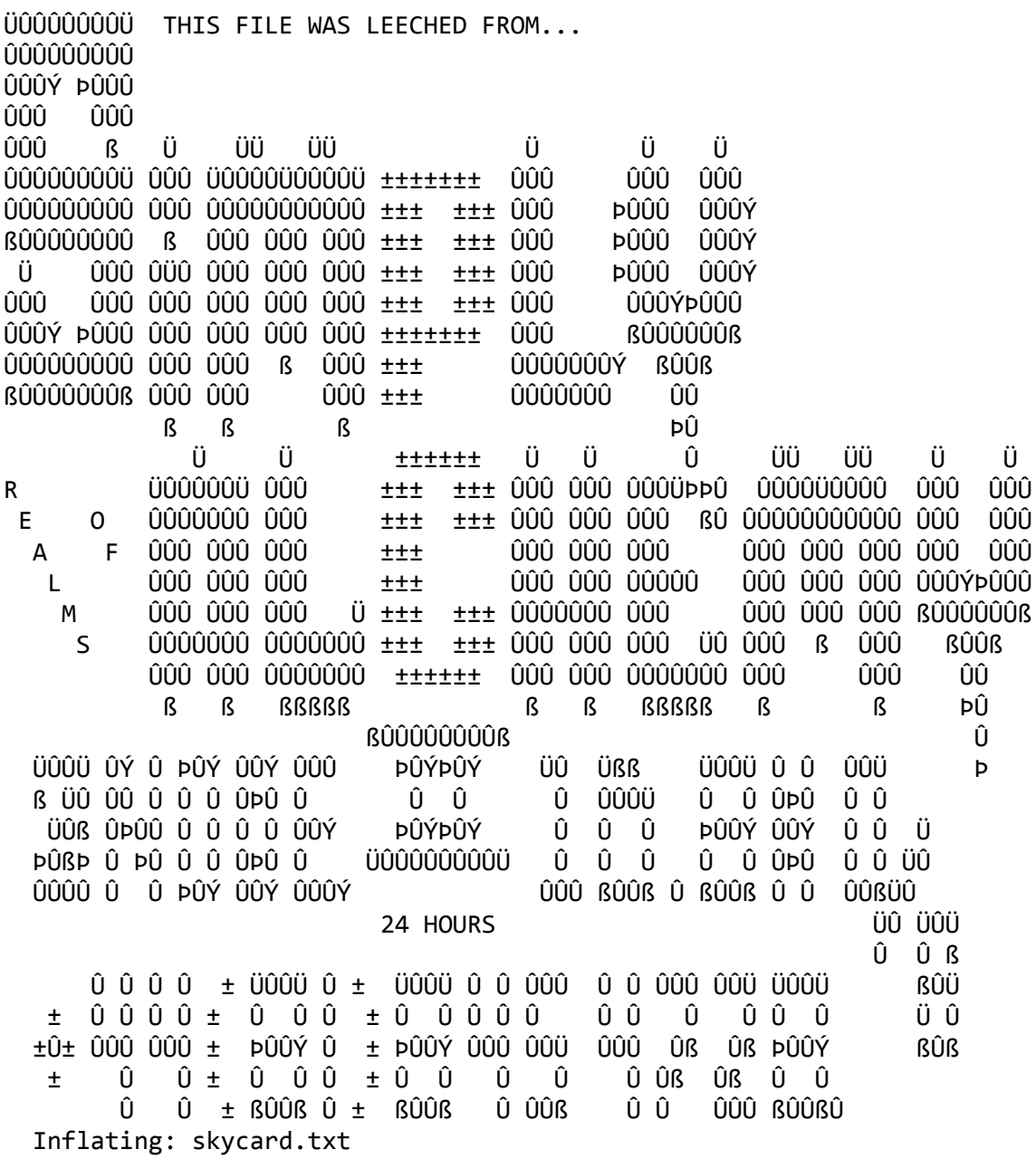


Inflating: skycard.txt

*** The Videocrypt System ***

An Overview

Researched and written by Darren Ingram, author of Satnews

- Satnews.. the latest and non-Commercial satellite news -

Version 1.31 - 06.05.91

Introduction

Videocrypt is a pay-tv scrambling system jointly developed by Thomson Consumer Electronics and News Datacom. Over one million users receive Videocrypt encrypted signals and this system, has to date, remained secure from illicit decoder manufacturers, protecting the revenue of Videocrypted television channels.

Requirements

Videocrypt is a multi-standard encryption system which is suitable for PAL, NTSC and SECAM transmissions. Language is no barrier for Videocrypt with its capacity for multi-lingual transmissions and broadcasts utilising a comprehensive on-screen instruction menu.

Features and applications

A smart card is the central key to the Videocrypt system, and the card can be used for a variety of diverse applications. The card is pre-coded to determine a users requirements and it can subsequently be addressed utilising the decoders logic to amend the users services at the broadcasters will.

There are a number of broadcasting modes which the smart card can be used within including:

Clear Mode
Signals sent in the clear are recognised by the decoder and passed to the display without further processing.

Free Access
Pictures transmitted with an encryption key are delivered directly to the display through the decoder.

Controlled Access
Access to encrypted pictures is determined by the level of access authorised to the users smart card. No signals will be transmitted in an unencrypted state without prior authorisation.

Programmes can be tailored to usage with the Videocrypt system and

the system offers a flexible way for pay-tv operators. There are a number of operations mode offered as standard including:

* Single or multiple subscriptions with many tier levels in one channel

* Pay Per View (PPV) and impulse purchasing

* Thematic selection (enable all arts programming)

* Geographic limitation (restrict to a country/area)

* Single-event (throwaway cards)

* Parental Control (reception with card only)

* Pre-determined time period

Videocrypt enables smart cards to be pre-programmed to suit the specific programming requirements.

Smart card - providing the revenue security

Security can be addressed on a multitude of levels when using the smart card. These include:

Chaining

An existing customer would receive a new card which contains part of the new code, the remainder of the code would be transmitted when the card is inserted into the decoder and the subscriber compiles with the instructions contained within the on-screen graphics.

Over-the-air addressing

Systems operators can now address individual subscribers, which is a vast improvement over other scrambling systems. The operator can provide additional services, reduce service entitlements, send individual messages, blacklist and/or whitelist viewers.

Cloning

A number of steps have been taken to stop smart cards being copied or cloned. A physical deterrent is the first line of defence, and the integrated circuit contained within the card makes "probing" very difficult as the IC is likely to become damaged in the process.

Cost is a second factor which is likely to deter manufacturers of

illegal decoders. A considerable amount of time, trouble and expensive resources would be required to clone the card.

The manufacturers of Videocrypt recommend that the cards are replaced every six months, and each time this is done a "secret encrypting algorithm" will be changed. Any pirate decoders manufactured during this time would be relatively useless.

And should a pirate decoder be manufactured, it will contain a unique security code, which could be blacklisted by the systems operator once the code has been discovered - leading to calls of complaint by angry customers.

Video taping

Videocrypt offers an simple method of tracking down pirates who video high-value programming and then distribute it.

The customers unique number can be displayed on the unencoded screen for reference and future litigation. Although an on-the-screen code can be generated for signals piracy in a public place, the codes can be hidden in the picture - and retrieved by a technician at a later stage.

Videocrypt-your flexible friend?

Videocrypt can be used in a number of applications other than tv signals protection. They include:

Messaging, messages can be transmitted to individual subscribers or to a group, so target messaging is now a potential. Messages like: "Satellite owners in LONDON call 081 XXX XXXX now for a great bargain".

Selling, sales over the air can be utilised with the unique identity number which verifies an owner and their registered address. Data can be matrixed with a user personality during ad-breaks to tailor-make the advertisement.

A unique transaction alphanumeric can be displayed on the TV screen, and the subscriber will telephone a given number and quote the alphanumeric - and the deal can then be completed in total security.

Scrambling

The majority of scrambling systems currently on the market are dependent on analogue processing circuitry, and it is a hard task to get a secure system without picture deterioration.

Videocrypt can encode and decode a picture without degradation.

The crux of the scrambling system evolves around a patented development of Active Line Rotation (Cut and Rotate principle).

Every line of the signal is cut at a number or points along its length, and this is chosen at random by a 60 bit psuedo random binary sequence generator (PRBS). As each cut point differs from the next the signal has no viewing value to an unauthorised recipient, but authorised recipients decoders recode the picture so that the true state of the unscrambled line is always first out for display.

The PRBS is re-seeded at times too, to enhance the security of the system even more.

Before this ALR process can take place, the decoder needs to be aware of the cut point on each of the transmitted lines, this is provided within the encryption process. Each decoder utilises an PRBS which reflects the characteristics of the system so that the two halfs can be synchronised and a viewable picture displayed.

Data is transmitted in a series of over-the-air packets, which looks like:

SYSTEM-----SMART or BLACKLIST

The system comprises of system data included Flat-Shamir identification information, on-screen display messages, fingerprinting and blacklisting data.

The smart card packet comprises of:

HEADER-----ENCRYPTED DATA-----CHECKSUM

The Videocrypt encryption system is based around a tightly-guarded secret which has defeated system hackers throughout the world. A final control algorithm is central to the systems security and this can be changed at will if the system has been hacked.

Complex calculations are performed within the system in order not to compromise its security.

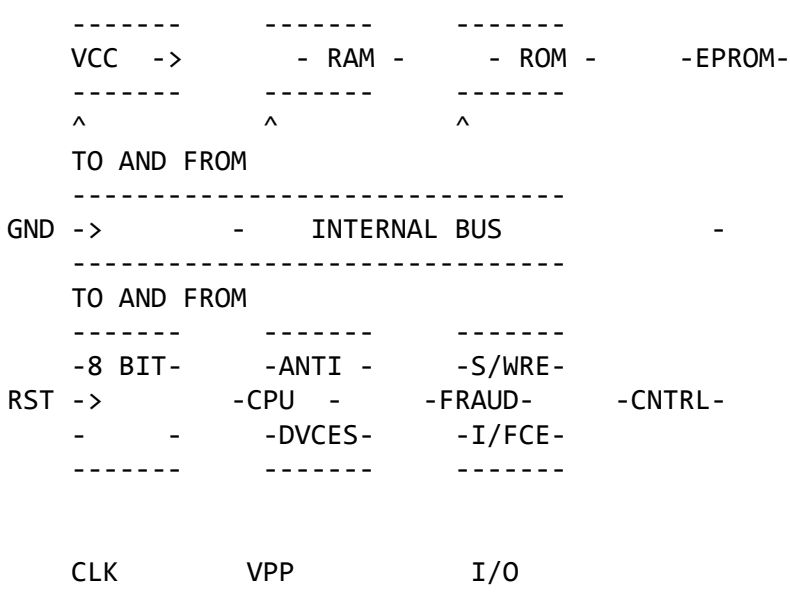
But hackers who have attempted to hack the decoder will be disappointed - as there are no secrets held within the system.

Smart Cards

The smart card offers great flexibility to the programme controller and the viewer alike, and is the key to the Videocrypt system.

The Integrated circuits incorporated within the smart card have a lot of power and contain EPROM elements which are partially burned during their manufacture. The ICs are buried within the design to make the system harder to penetrate.

Smart card block diagram



Over the air addressing

Algorithmic information is transmitted to the viewer over the air, encrypted within the Videocrypt system.

This data is transmitted within the Vertical Blanking Interval (VBI) and four lines are employed for active data and two others, one white and one black (for test purposes).

An application of Non Return To Zero (NRZ) with an constant energy spectrum maximises the systems characteristics.

Four picture-sustaining techniques are used to ensure a high quality picture. Bit interleaving, hamming codes, quadruple repetition and check sums are used within the process.

The system can cope with fringe reception areas and will still function correctly with high levels of noise.

Picture quality

Picture quality is paramount for any scrambling system and due to the standard being of a digital origin, integrity of the signal is maintained throughout the encryption and de-encryption process. Amplitude sampling is conducted by the decoder and a 14MHz internal clock ensures jitter-free pictures and unstable framing. A digitally derived Automatic Gain Control (AGC) is also included within the receiver.

Scrambling Sound

Videocrypt also has the capability of encrypting sound sources to enhance the security of premium events. To date this level of security has not been utilised by broadcasters.

The system of spectrum inversion renders the sounds received without authorisation worthless. Videocrypt transposes the frequencies transmitted and this in turn removed distortion of the sound.

Technical Data
(supplied by Thomson Consumer Electronics, 1991- subject to change)

VIDEOCRYPT BASEBAND DECODER
* Stand alone video decoder
* On screen display
* De emphasis switch
* Authorise button
* Integrated smart card reader
* Power indicator

PAL MODEL

Video input level	IV +/- 3dB flat and clamped
Baseband input level	250 mV +/- 3dB, unclamped level measured at pre-emphasised transition frequency
Suitable de-emphasis	CCIR 405-1
Video output level	IV p.p. into 75 ohms
Video bandwith	50Hz - 4.8 Mhz -3dB typical
Line tilt	<_ 1% typical
Luma/Chroma Delay	+/- 50nS typical
S/N ratio:	50dB typical weighted

CONNECTIONS

AV Peritel (Scart)	
Audio loopthrough	Left and right
Pin 8	High with scrambled video input Low with clear video input

Pin 16	5v 50mA maximum for external modulator (OPTION)

MISCELLANEOUS

Standards	Designed to IEC 65
Operating Temperature Range	5-40 C
Mains Input	216-255 V AC 50 Hz
Power Consumption	15W
Weight	2.5Kg

VIDEOCRYPT ENCODER (PAL/SECAM/NTSC)

* 19" rack mounting
* Active line cut and rotate
* Twin or single scrambler
* Separate power supply
* Integrated cooling unit
* Data for control access in the VBI
* RS232 interface

Video input level	IV 75 ohm
Video output level	IV peak to peak +/- 2% 75 ohm
Line tilt	0.5% typical
Base line distortion	0.5% typical
Chrominance to luminance	3% typical
2T/Bar ratio	2% typical
Synchro level	1% typical
S/n ratio RMS weighted	>_ 67dB
Chrominance luminance:	
intermodulation	<_ 2%
differential gain	1% typical
differential phase	1" typical
luminance non-linearity	1% typical
chrominance/luminance delay	+/- 10nS typical
video bandwith at 3dB	>_ 5.8 Mhz
Output DC level	300 mV +/- 50 mV
Sampling frequency rejection	>- 50dB at 14 Mhz
Number of bits per sample	10

CONNECTIONS

Connections to security comp	RS232
Local VT100 terminal	ditto
Video in	BNC 75 ohm
Scrambled video out	BNC 75 ohm

MISC

Local terminal functions are to
show working parameters
give warnings

control local
remote
autonomous
Select scrambling mode
clear
free access
control access

Mains input low pass filtering
Audio scrambling using spectrum
inversion 0dB/600 ohm (optional)

ENDS

**** Sky card hacking info 26/06/1993 ***

When the VideoCrypt system was launched, the press releases claimed that it was the most pirateproof system yet devised. Some of the people involved in the design of the system claimed that it would take billions of years to break the codes used by the system. The usual media journalists swallowed this hook line and sinker. The hackers knew otherwise.

The VideoCrypt system is the mainstay of the BSkyB satellite television empire. It is the means by which BSkyB makes its money from the subscribers. The basic theory is that they pay a subscription for the premium channels and they receive a smart card. This smart card, when inserted into the VideoCrypt decoder will allow the decoder to descramble the channels paid for. It is also possible for BSkyB to turn off the cards of those subscribers who have not paid.

Hacking scrambling systems such as VideoCrypt is a multi-million pound industry. Due to the present legal situation it is perfectly legal to hack a channel that originates outside the UK. However for someone in the UK to hack a UK originated channel is illegal. Such mere facts as illegality have never bothered pirates.

In the last few weeks the impossible has happened. The VideoCrypt system has been conclusively hacked. It is now possible to purchase a pirate smart card or chip which will allow the viewer to descramble Sky Movies Plus, The Movie Channel, Sky Gold, Sky Sports and TV Asia. The cost of this pirate card is œ99. The price in itself is lower than the subscription for the channels.

Other channels using the VideoCrypt system. Are worried. According to the latest reports, The Adult Channel and JSTV have been compromised as well. This means that all of the channels currently using the VideoCrypt system as a fee gathering system have just lost control of the market. It is now, well for the moment anyway. a pirate's market.

This hack is, like all hacks, colourfully named. It is known as the "Ho Lee Fook" hack. The joke being that this is generally the exclamation uttered by people when told of the hack. There are two forms of the hack; a card and a chip.

The card version of the hack is about sixteen millimetres longer than the official BSkyB card. Essentially it is a single chip mounted on a printed circuit board that plugs directly into the VideoCrypt decoder's card socket. This is the more user-friendly version as it does not require any modification to the decoder.

The chip version does require some modification to the decoder. The official VideoCrypt name for the chip in the decoder is "The Verifier". This chip has to be removed and replaced with the pirate chip. The decoder will then decode the scrambled channels without the need for the BSkyB smart card.

The pirate cards and the chips are on sale. It is believed that a number of them are already in the UK. Indeed I received one, in a brown paper envelope, on June the eighth. It is still working.

The problem for BSkyB and other users of the VideoCrypt system is not one of containment. Things have progressed too far for that. The problem is more serious. Unless they can come up with a quick fix for the system that will render the Ho Lee Fook hack inactive, they have to replace the smart cards.

BSkyB initially set out to replace their smart cards every three months. This continual update was, so the theory went, meant to deter hackers from trying to hack the system. Fiscal reality has a crushing effect of such business school theories.

VideoCrypt suffered its first real disaster when someone discovered that by limiting the programming voltage to the card, it was possible to stop the card being switched off. This hack was known as the "Infinite Lives" hack. It was an old computer term for a modification to a games program that gave the player unlimited lives. Since BSkyB could not turn off the cards it seemed an apt name. This hack was followed by a new issue or batch of cards. The "Infinite Lives" hack did not work on the new cards

but a new hack did.

The KENtucky Fried Chip upped the ante. It was the first time that the actual internal operation of the VideoCrypt decoder was interfered with. It was a rewritten "Verifier" chip that was programmed to stop the cards being turned off. It did not work at full efficiency so it was not marketed by the pirates. After this hack, BSkyB issued a new batch of cards which was more resilient to this hack.

The current card issue is issue 07. The Ho Lee Fook hack is working on this batch. If BSkyB introduce issue 08 cards, then there is the possibility of the hack ceasing to work. At this stage there is the terrible spectre of the hack being updated to work with the 08 cards. It is the thing of which BSkyB's nightmares are made of.

The issue of new card batches occurs mainly in Spring or Autumn. A Summer launch of the new 08 cards would be unusual. As VideoCrypt will be going to a tiered channel structure in the Autumn, it would seem that they have planned an Autumn update. The Ho Lee Fook hack may force them to bring their plans forward by some three months or so.

The confidence in a system is not based on how well a system repels hacks but rather on how well a system recovers from hacks. This will be a true test of the VideoCrypt system and its smart card based philosophy. The philosophy is that of the detachable secure controller. Basically what this means is that if the system is hacked then all that needs to be done to stop the hack is to issue a new card.

The effects on the confidence of present and prospective users of VideoCrypt is more difficult to gauge. The smart card is the core of the VideoCrypt system. Seeing it replaced by a pirate smart card contradicts every claim made in favour of VideoCrypt. It was not supposed to be possible. One thing is certain, channels will now have to look at a scrambling system as only being a temporary form of protection that has to be frequently updated. Failure to do so will be fatal.

John McCormac
Author of "European Scrambling Systems 3" ISBN 1-873556-02-0
Editor of Hack Watch News.---

*** Latest ***

There is no such thing as coincidence - or is there? On the day that the film "Sneakers" was released on video, I received an actual working hack for the scrambled Sky channels. The film "Sneakers" is about events surrounding a piece of equipment that can hack any cryptosystem. The piece of equipment that I received is essentially a chip that can hack the Sky VideoCrypt channels.
This latest hack on the VideoCrypt system has been labelled the "Ho Lee Fook" hack. The reason for this name is more to do with people's reaction to the hack rather than its origin, which incidentally is Central Europe.
This is perhaps the most dangerous hack to have occurred on VideoCrypt - it replaces the smart card. In effect it is a new smart card that gives access to all the Sky channels. Of course the problem for Sky is that it is not a genuine Sky card.

The card is approximately sixteen millimetres longer than the official Sky card. It is a blue printed circuit with a single surface mount chip, and five connector pads. The identification numbers on the chip have been scrubbed.
The standard check for a card of this nature is to look for a wafer from an official smart card. In the early days, a fairly common scam was to take the chip and connector pad from a valid Sky card, trim away the plastic and then put the chip in a DIL header. The DIL header would then be blobbed in a lump of black resin so that it looked like an IC. The decoder would then have its card reader replaced with an ordinary DIL IC socket. Then the decoder and chip would be shown or sold to some unsuspecting, if greedy, punter.
The chip appeared to be real, with no wafer underneath the body of the chip. The actual stubs of the chip die were just visible at the end of the chip. It was a genuine chip.

It has been working steadily for the last few days and there appears to have been no kill messages sent to it. If it had been a direct clone, Sky would have been able to kill it over the air - or would they?
Since the people who developed this hack obviously understand the operation of the over the air addressing, they may well have designed a filter to stop the kill message from having any effect of the pirate card. There are of course more devastating implications here. The card itself may only contain the data and algorithms necessary to descramble the signals.
The chip version of this hack is based on the 8752. This Ho Lee Fook chip will replace the official 8052 in the decoder. A selling price of ninety nine pounds has been mentioned in Germany.

Nobody is sure what the people in News Datacom are doing about this hack. Sky are more than likely very upset that someone has hacked their pirateproof system yet again. This is the fifth hack and the image of a

pirateproof system now only exists in the minds of PR people.

*** -=Y_HS=- all (c)'s acknowledged ***