

The offering of navigation devices at discounted prices by MVPDs is ultimately pro-consumer. MVPDs have every incentive to get high-quality navigation devices into the hands of their subscribers at attractive prices in order to best be able to provide and market a full range of services to these subscribers. Low price, high quality devices thereby benefit the consumer and the MVPD, particularly as competition between MVPDs for new service offerings and network features becomes more dependant on the capabilities of innovative technological developments.

Indeed, in the near future, with the rollout of digital services and equipment, discounted equipment offered directly by MVPDs will assist the transition of their networks to digital transmission, and will eventually hasten the successful development of digital television. Discounted equipment will ensure that an MVPD can establish a minimum subscriber base that makes the offering of new digital services more economically viable. On the other hand, without the ability to offer subscribers direct incentives to switch to digital equipment, there may be an insufficient subscriber base to support offer digital services and programming, and attempts to offer all digital services would be hampered.

Equipment discounts should only be a concern where they are not real discounts, but rather where the cost of the equipment is hidden in a long term programming service agreement. Such so-called discounts are in fact offset by service rates over the length of the contract. As the NPRM recognizes, a perfect example is the deep equipment discounts currently offered by DBS providers for their equipment.^{62/} Many DBS providers subsidize the sale of video decoders and dishes at low prices in exchange for long-term service contract

^{62/}NPRM at ¶ 42.

commitments from subscribers. Such discounts are not real discounts but are instead precisely the type of subsidies that Congress was concerned about because they create disincentives for subscribers to switch MVPDs, thereby forestalling both MVPD and equipment competition.

Accordingly, to carry out the intent of Section 629(a), the Commission should prohibit all MVPDs from offering any equipment discounts tied to long-term programming service agreements. If, on the other hand, DBS providers and certain other MVPDs are allowed to continue to link equipment discounts to long-term service contracts, there is no rational basis for not allowing all MVPDs to have the very same flexibility.

VIII. DEVELOPMENTAL WAIVERS.

In directing the Commission to provide for broad developmental waivers for newly emerging technologies and services, Congress recognized that development and successful introduction of new services will often require waivers of any navigation device rules adopted.^{63/} Time Warner agrees that the on-going development of innovative services provided over MVPD networks demands that the Commission liberally grant such developmental waivers. In the long run, liberal use of such waivers will allow MVPDs to roll out new services and products in a manner that best suits consumers' wants and desires, promotes the most efficient use of MVPD networks, and thereby assures that the public interest is best served.

There are many important reasons for the Commission to view requests for such waivers sympathetically. Most importantly, new service offerings often require the

^{63/}See 47 U.S.C. § 549(c).

development and deployment of proprietary equipment designed to support such services. This new equipment often poses unique technical network security problems which can not be dealt with until a full-blown trial of the new service is initiated. Indeed, with any new service using a broadband network in a revolutionary way, and especially interactive two-way services, there are bound to be unforeseen network security issues that arise. Test equipment that is under the exclusive technical control of the MVPD is essential in order that any such problems can be dealt with quickly and in a controlled manner.

Furthermore, the introduction of new services often requires marrying a particular service to a particular piece of hardware until the service has successfully established itself. Indeed, many services will require certain economies of scale which dictate that a given level of subscribers take the service before an MVPD can even begin to determine whether the service will ever become economically viable. Retailers and independent equipment sources are unlikely to manufacture such a test product before the economic viability of the underlying service is firmly established. MVPDs must therefore be able to test market the service and offer the equipment to allow the service to reach a certain critical mass before the service or the product will ever be successful.

Time Warner recommends using a waiver approach that is procedurally consistent with the waiver request procedure applicable to cable systems.^{64/} Parties requesting a waiver should be required to submit a showing demonstrating the general technical characteristics of the trial, and provide a showing that the public interest would be served by grant of the waiver. After the waiver request is placed on public notice, twenty days from

^{64/}47 C.F.R. § 76.7.

the date of public notice is sufficient time for interested parties to comment, and 10 days from that point is sufficient time for the petitioner to reply. The burden should be placed on any party seeking to oppose the introduction of new services and technology to show why grant of a waiver would not be in the public interest. The Commission at this point should not establish specific substantive standards for granting such waivers. Consistent with Congress' directive that waiver requests be decided within 90 days of filing, any developmental waiver application should be deemed granted if not otherwise acted upon within 90 days.

The term of any waiver should last for the useful life of the equipment involved, or the investment payback period, whichever is longer. Furthermore, the Commission should allow any waiver to become permanent where the applicant agrees, after an appropriate introductory period, to license its product for manufacture by third parties. Such an approach provides the best incentives for manufacturers to cross-license proprietary technologies, while also protecting the ability of MVPDs to test such services and equipment.

IX. ALL RULES ADOPTED PURSUANT TO SECTION 629 SHOULD SUNSET ON A NATIONAL BASIS.

The Commission proposes that the sunset provisions contained in Section 629(e) of the Communications Act "should be read as flexibly as possible."^{65/} Time Warner agrees that the sunset provisions should be interpreted flexibly in light of Congress' express preference, in enacting the 1996 Act, for marketplace solutions over regulation. Indeed, the preference for competition over regulation underlies the entire structure of the 1996 Act, and

^{65/}NPRM at ¶ 82.

the legislative history makes this abundantly clear. For example, the Conference Report states, on the very first page, that the purpose of the 1996 Act is "to provide for a pro-competitive, de-regulatory national policy framework designed to accelerate rapidly private sector deployment of advanced telecommunications and information technologies and services to all Americans by opening all telecommunications markets to competition."^{66/}

The Commission initially proposes to consider relevant geographic and product submarkets in determining the presence of competition for purposes of the Section 629(e) sunset provisions.^{67/} This proposal is entirely misguided and overcomplicated. The realities of the marketplace dictate that all rules adopted pursuant to Section 629 should sunset on a *national* basis when the Commission determines that the factors of Section 629(e) have been satisfied. Indeed, in practice, any equipment sold for use with MVPD service is likely to be made available on a *national* basis.

Accordingly, in determining under Section 629(e)(2) that "the market for converter boxes, and interactive communications equipment . . . is fully competitive," the Commission's inquiry must focus on the *national* level, and not on an attempt to analyze submarkets, which would inevitably be arbitrary and require time-consuming presentations of evidence. In sum, any attempt to define local "markets" or "submarkets" for navigation equipment or MVPD competition will result in unnecessary confusion. Competitive realities dictate that all rules adopted pursuant to Section 629 should sunset on a national basis when the Commission determines that the sunset criteria contained in Section 629(e) have been satisfied.

^{66/}Conf. Rep. at 113.

^{67/}NPRM at ¶¶ 50-51, 82.

X. CONCLUSION.

Implementation of Section 629 of the Communications Act will not be an easy task. Rapid technological advances and emerging competition in the provision of MVPD services require that the Commission maintain a flexible approach to assuring that navigation devices intended for use with MVPD systems become commercially available. Consistent with the statutory directive, the Commission should work closely with industry organizations to develop equipment and service criteria that will reflect marketplace realities and intervene in the process only when necessary to ensure that progress continues to be made in interindustry attempts to resolve the many complicated technical and service issues that can and will arise. Above all else, the FCC must be faithful to the Congressional admonition that the security of MVPD services not in any way be jeopardized by regulations adopted to foster the commercial availability of navigation devices.

The key to maintaining the appropriate balance between the desire to achieve commercial availability and the need to protect signal security requires: (1) removing security functions (both conditional access and decryption) from commercially available navigation devices; (2) allowing distribution of equipment performing security functions to be strictly controlled; (3) ensuring that all commercially available equipment has a minimum level of functionality that will support the services and features offered over the MVPD in a hardware transparent manner and that will not allow the copy protection technologies employed by the creative artists or service distributors to be bypassed or defeated; and (4) establishing expedited procedures to halt the commercial availability of any device causing harm to MVPD networks or being used to facilitate theft of service.

In these comments, Time Warner has identified specific issues that must be resolved as the Commission moves forward to implement the statutory mandate. In each case, Time Warner has attempted to set forth specific policy approaches and regulatory guidelines that will enable the Commission to carry out its difficult task in a manner which successfully balance the interests of service developers, distributors and consumers. With a creative and flexible approach, and careful accommodation of the legitimate interests of all parties involved, the difficult issues faced by the Commission in this proceeding can not only be solved in a satisfactory manner, they can be solved in a manner which will benefit all.

Respectfully submitted,

TIME WARNER ENTERTAINMENT COMPANY, L.P.

By: Arthur H. Harding

Aaron I. Fleischman
Arthur H. Harding
Howard S. Shapiro
Craig A. Gilley

Fleischman and Walsh, L.L.P.
1400 Sixteenth Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 939-7900

Its Attorneys

Dated: May 16, 1997

EXHIBIT A

System Hack

Has DSS Been Hacked?

By John McCormac - Editor Of Hack Watch News

According to available information, the Digital Satellite System smart card has been hacked. The pirate cards will enter the market in soon. The price for the basic tier pirate card will be \$150.

Four tiers of pirate cards are planned. The first tier will only include the basic programmes. The second tier card will include the subscription movie channels. The third tier card will give access to the sports packages. The last card will give access to all services and will include a ceiling of \$500 in Pay Per View credits.

The best description for what is in formation is an "Alternate Access Control System". The pirates will be supplanting the official DSS management with their own. Subroutines that marry the pirate card to an individual IRD will be included to prevent or at least deter piracy of the pirate card.

This has been a major problem in Europe. The majority of the pirate smart cards for VideoCrypt are based on the PIC16C84 microcontroller. Despite its security, this chip was popped and the programs are routinely extracted. As a result of this, the program for hacking VideoCrypt spread rapidly throughout Europe. A repeat of this situation is the last thing that the DSS pirates want. Therefore they may go for a more secure processor. Some sources have commented that one of the Dallas microcontrollers or the new Zilog microcontrollers might be used.

The main pirate operations will take place outside the USA. Canada has been mentioned as one particular site. Others sources have mentioned islands in the Caribbean. Piracy of satellite television signals is a serious business in the US for the channels, the pirates and the Law.

The Hack And How It Might Have Happened

You have got to wonder at the kind of mind that would put a patent number on a smart card. It is just like telling a burglar what kind of lock your door uses. And yet this is exactly what has happened with the DSS card. The text that appears on the card is as follows:

'This card is the property of News Datacom Ltd. and must be returned upon request. Incorporates Videoguard (tm) security system. Provided for reception of authorized 101 W longitude satellite services. Protected by U.S Patent 4,748,668, and others.'

That patent referred to on the smart card is the Fiat Shamir Zero Knowledge Test. It is an authentication algorithm that the decoder runs to see that the smart card inserted is a genuine smart card. The same authentication algorithm is used in the analog VideoCrypt system in Europe. This may not be the only commonality. To understand what may have occurred, we have to go back to early 1994.

In Europe, the VideoCrypt system, using the issue 07 card, was hacked. The full source code of the hack had been distributed freely on the Internet and via BBSes. The Digital Satellite System was preparing for launch in the USA. It was gut wrenching time for the executives in DSS. The common element between Europe and the US was News Datacom. The DSS executives were worried about the security of their new system. Would what happened in Europe happen in the US?

Slowly but surely the press barrage started. The satellite television trade press began to run articles about the new DSS system. They were, in hacker terms, content free text. The majority of these articles were written by clueless people without any knowledge of what really happened in Europe. One article in particular stated that VideoCrypt had been unhacked since its introduction in Europe in 1989. Yeah right! And the 500,000 Pirate VideoCrypt smart cards and the Omigod emulator programs did not exist. It was a replay of what had happened in Europe - the puff pieces in the trade press and the inevitable hacks.

Well the 500,000 pirate VideoCrypt cards were very real and they forced Sky to issue their new card ten months ahead of schedule. There was an even greater problem. The 08 card they had planned to launch was almost identical to the hacked 07 card. Instead they had to go for the 09 card.

The 09 Sky card was different from the 07 in two major ways. It had a different architecture and it had a very different algorithm. Sky started to distribute this new card in February 1994 but they did not switch over to the card until 18th May 1994. That day is known as Dark Wednesday by European hackers.

The connection here is the timing. It would have been very convenient for News Datacom to draw heavily on the Sky 09 card for the new DSS card. Most of the ROM routines could have been easily adapted for the new system. The main changes would of course have been in the EEPROM. The EEPROM of the smart card is the area that contains the main cryptographical routines.

The operation to pop the 09 Sky card in Europe took a few months. It involved completely reverse engineering the smart card. Some preliminary code was sold in June last year at an auction in London. It was a start but it took a further four months before the system was totally compromised. Perhaps the most important part of the operation was the discovery of a back door in the smart card's code.

When VideoCrypt was developed, the overall structure of the system was, compared to systems like VideoCipher II, simplistic. It was also reliable. But the designers may never have expected it to be handling over two million subscribers.

As a direct result of this loading, the designers of the system, News Datacom, had to incorporate some newer levels of access control into the system. Upgrading the decoders was out of the question. There were too many and it would be very difficult to track all of them down. Most of the standalone decoders had long ago disappeared into Mainland Europe.

News Datacom's solution was clever and at the same time extremely stupid. They incorporated a method of programming the card over the air into the code of the 09 Sky card. The over the air instructions were included in the standard access control data packets. They looked just like more card identity numbers but they were not. The hackers labeled them "Nanocommands".

The over the air programming scheme was clever in that it gave them more control over the cards - they could easily implement ECMs by updating the card's EEPROM and they could actively change the channel authorization. In effect they could even run a limited form of Pay Per View.

Of course there is a downside. All of the security of this card relied on the hackers not finding out the core algorithm and obtaining a working knowledge of the card addressing. The core algorithm had been sold at auction in June 1994. The rest was only a matter of time.

The cracks in the edifice were beginning to show. By the end of July, VideoCrypt was crumbling. The Phoenix hack had worked. This hack relied on an understanding of how the access control data packets were

encrypted and structured. (The Phoenix hack allowed hackers to activate or reactivate all channels on Sky cards using a computer and eventually a standalone programmer)

Naturally when Sky tried to retaliate against the Phoenix hack, they used the Nanocommands. The hackers were watching. It was true electronic warfare. Sky and News Datacom versus the hackers.

Gradually the function of each nanocommand was ascertained. Even now it is difficult to believe what happened next. One was found to read a byte from the EEPROM as the input for a round of the algorithm. Another of the nanocommands was found to act like a BREAK command. It would dump the current result out as the key.

The hackers had the algorithm and knew the result just prior to the byte from the EEPROM being used. They could dump out the the result just after the EEPROM byte had been processed through the algorithm. Since they then had the main components, it was simply a case of starting the algorithm from the first result and stepping through the values 0 to 255 as the input byte. The hack has become known as the Vampire Hack.

Of course this attack was not perfect. The resulting data from the Vampire hack of the 09 Sky card did not make sense. The processor used in the smart card was based on the 6805 but the data was definitely not 6805. There was a little bit more decryption to be done yet. But eventually it the hackers cracked it.

Now what happened with DSS? The speed of the hack seems to strongly indicate that the same card type was used for the DSS system. This would mean that the same techniques that were used to pop the 09 Sky card could be employed on the DSS card.

The real test of the pirate cards lies ahead. As with the European VideoCrypt, the DSS smart card may be over the air programmable. This would mean that DSS could update their cards over the air without having to immediately issue new cards. The pirate cards would of course require upgrading.

The main difference is that the American hacking industry has experience of such upgrading. The technology used to hack VideoCipher II can be used for this upgrading. The pirate cards may well come with a modem module that can be used to automagically update the card.

[Back To Main Page](#)

Copyright (c) 1995 Hack Watch News

Analysis

Hack

Piracy

Satellite Piracy - *The European Experience*

By John McCormac - Editor Of Hack Watch News

In mid-1994 the RCA digital satellite system (DSS) was introduced. The system is digital and therefore takes advantage of compression techniques to squeeze a number of channels into the bandwidth that would normally be occupied by a single satellite TV channel.

The DSS is currently transmitting from a pair of co-located satellites at 101 Degrees West. Since the satellites used are transmitting on a higher frequency with higher power, the size of the dish is also smaller. It is only the size of a pizza pan - about 18 inches in diameter. Currently there are about 150 channels being transmitted. More will be added. But something from the past is worrying people - piracy!

In the late 1980s and early 1990s piracy haunted the large dish C- Band satellite television. Could the same thing happen to the DSS system? Only time will tell. The DSS encryption is based on the VideoCrypt access control system. The European analog version of VideoCrypt has been repeatedly compromised by hackers over the last five years.

Europe - The Present Situation

There are three main scrambling systems in European satellite TV. The first and most obvious is VideoCrypt. This system is used by BSkyB and a number of other channels. (BSkyB is the broadcaster of the Sky Multichannels Package which carries three movie channels and a few general entertainment channels for the Irish and UK markets) There are an estimated 2.5 Million Sky subscribers using VideoCrypt smart cards to gain access to this programming.

The second principal system is EuroCrypt-M. It is used by Canal Plus, TV3, TV1000, FilmNet and a few others. There may be as many as 400,000 satellite subscribers to these channels. The market for these channels is mainland Europe and they have many more subscribers on cable. The third scrambling system is Nagra Syster, the only one that is still secure from signal hackers. It is used by Premiere, Canal Plus and Teleclub. While hackers are actively working on a viable hack, the system has fared well during the past four years.

One major difference between between Europe and the United States is the uniformity of American laws and their enforcement. Piracy has thrived in Europe because each nation has its own copyright laws and generally only protects its own channels. This makes it possible, for example, to legally sell pirate smart cards that allow access to BSkyB's VideoCrypt encoded channels throughout all of Europe except in the United Kingdom (UK).

The VideoCrypt system as used by DSS in the United States differs from the European implementation. The European implementation is a purely analog system that only scrambles the video. The DSS is a completely

digital system that encrypts the digitally encoded video and audio. However there are some similarities. The most obvious is the smart card.

The European VideoCrypt system, like DSS, is based on a secure detachable processor - the removable smart card holds all of the critical data. The smart cards are both the systems' greatest strength and weakness. Smart cards permit the broadcasters to change or upgrade their conditional access system. In small quantities it can be relatively inexpensive but when there are a few million cards to be replaced, the costs increase. BSkyB paid 21 Million pounds for their last card change. Originally they had planned to change their cards on a three to six month cycle. Unfortunately when they changed their cycle, they gave the hackers enough time to hack the smart cards.

DSS faces a similar threat. Since the VideoCrypt system in Europe has been totally compromised, European pirates have already set their sights on DSS. Some sources have reported that DSS has, indeed, been hacked already and that pirate cards will be on the market by August. Even if it proves untrue, European hackers have an intimate understanding of the VideoCrypt system and it is a good starting point for a hack on DSS.

What Is VideoCrypt?

The European implementation of VideoCrypt is a video only scrambling system. The active video section of each line is cut and rotated about one of 256 points. The cutpoint for each line is generated from the output of a Pseudo Random Number Generator.

The seed for the PRNG is derived from the data transmitted over the air along with the video. The decoder extracts and passes this data to the smart card. The smart card runs the seed generation algorithm and returns the correct seed to the decoder. The decoder itself is essentially "dumb" because the main cryptography takes place inside the smart card.

VideoCrypt decoders contain a few built-in algorithms to stop pirate card from being used in the decoders. However due to a programming error on many of the original decoders and IRDs (integrated receiver-decoders), the most powerful algorithm, the Fiat Shamir Zero Knowledge test, did not work properly. Although the same authentication algorithm as used in the DSS system, it is doubtful that the same error was made.

The Fall Of VideoCrypt

VideoCrypt was hacked in fifteen seconds because it contained a fundamental flaw that was common to most of the smart card based systems designed in the 1980s. The data flow between the card and the decoder could be tapped just like a phone conversation. The data could be fed to other decoders and they could all decode the programming from the data produced by the one authorized card.

This hack, presented in a article written about the security of smart card based scrambling systems, is known as the McCormac Hack. It works and is in operation in Spain where it is feeding an MMDS (multipoint microwave distribution system) network from one smart card.

The ease with which VideoCrypt could be hacked was terrifying. Here was this system that was advertised as the most pirate-proof system yet developed and it was hacked. It was only the beginning of the nightmare for Sky and News Datacom.

The Infinite Lives Hack

Another major hack on the security of the VideoCrypt system was the Infinite Lives hack. At the time, the smart cards were using EPROM technology. These cards needed 21 Volts to program them. By limiting this voltage to 12 Volts or so, it was possible to prevent Sky from reprogramming or turning off the cards. (This is a variant of the hack on the France Telecom phone cards where the programming voltage pad was covered so that the payphone could not overwrite the card.)

The KENtucky Fried Chip Hack

The KENtucky Fried Chip was named after Ken Crouch, the head of Sky's Security Department. The hackers had modified the program in the IC that controlled the smart card interface. It would read the identity of the smart card inserted in the decoder. Then it would look to see if there was a kill message addressed to that particular card and if there was, the modified program ensured that the kill message never reached the card. This technique of modifying the operation of an IC in the decoder is known as "chipping" in the US. It was the first incident of this type of hacking in Europe. In the DSS system, the smart card interface is controlled by a custom microcontroller.

The Ho Lee Fook Hack

The name of this hack on VideoCrypt is more to do with the exclamation uttered by people told of the hack. It was a direct replacement for a smart card.

The first version drew heavily on the KENtucky Fried Chip hack. It modified the same chip so that it contained the same algorithm as the authorized smart card. Thus the first cardless Sky VideoCrypt decoder was born - something considered impossible by News Datacom. They had used Fiat-Shamir's Zero Knowledge Test and had integrated into the VideoCrypt system for just such an event. Strangely it never worked.

This first version of the hack was too insecure and too expensive. The solution was in a low cost microcontroller known as a PIC. The PIC controller range is manufactured by Arizona Microchip. They are RISC microcontrollers and as such can give a superior performance over conventional microcontrollers in certain applications. Pirate smartcards happened to be one of these applications.

In early June 1993, the first PIC smart card was developed. It was coded up on a wet Saturday afternoon somewhere in Europe. This was now a genuine pirate smart card - the very thing that the brochures on VideoCrypt said were impossible. Sky's VideoCrypt was to remain completely smashed for approximately one year - the remaining lifetime of the Sky's 07 card.

All of the Sky channels, and almost every other VideoCrypt encoded channel were available from the pirates. The minor electronic countermeasures (ECMs) that News Datacom implemented were easily dealt with by hackers often within a few minutes.

A leap in hacking technology had been made. The newer versions of the pirate cards were reprogrammable. With a modem it was possible to transmit a card update to all the European dealers within a few hours.

Since their technological attempts to control hacking had failed, Sky and News Datacom sought help from the Law. At first they attacked the pirates in the UK but then stupidly moved to Ireland.

VideoCrypt - The Irish Court Case - A Question Of Copyright

The law was cut and dried in the UK. Fortunately Ireland is not part of the UK. A major precedent was set when Sky tried to pursue David Lyons of Satellite Decoding Systems, an Irish based business, through the Irish courts. Sky alleged that the copyright of the software in their Sky smart card had been infringed.

Through a combination of technological ignorance and reluctance, Sky were defeated. They never provided any proof that the copyright of their software had been infringed. They claimed that since both cards decoded their channels, it was obvious that it was their software in both cards. It was pointed out that $2+2=4$ but so does $1+1+1+1=4$. They failed to distinguish between the output of the software and the actual software. The Judge ruled against Sky.

The TV-Crypt

Perhaps the most significant event of 1994 in the hacking world, was the formation of the TV-CRYPT. It is a non-commercial group interested in exploring scrambling systems. In some respects it is like the DESUG that was formed to hack the VideoCipher II in the mid 1980s. This is where the Omigod hack originated from. It is also where the Phoenix hack was stolen from.

When Sky One was scrambled in September of 1993, many European viewers were cut off from watching Star Trek - The Next Generation. The final season, Season 7, was about to be shown on Sky One. A high proportion of hackers watch Star Trek. What followed was only logical.

The logical answer was an emulator program for the personal computer to drive the decoder. Some of the commercial hacks were examined and in one case the code was extracted from one of the Ho Lee Fook chips. The code from the 8052 microcontroller was transcoded into C. From there it was transformed into the PC program known as Season 7 or Omigod. The pronunciation is Oh My God!

The distribution of the Omigod hack only took a few hours. It was available on all major BBSes and at many internet sites in Europe. There were even copies floating around at the Cable And Satellite Show in London, one of the biggest trade shows in Europe. Most of the top hackers in Europe were together in the same place at the same time.

Dark Wednesday - Sky Switch To 09

The reality of the situation was beginning to tell on Sky. They could no longer evade the problem and they switched to their new smart cards - issue 09. Although Sky had been sending these cards out since February it wasn't until May 18th that the pirates cards ceased to operate. The Omigod program stopped working. Sky had, or so they thought, won the war. The fun had only just begun.

The Great Code Auction

Something decidedly strange happened on June 20th. There was an auction in the Dorchester Hotel. Sky's 09 code was being auctioned off. More importantly it worked. Sky's smart card was compromised again.

It is not known how much money changed hands but the theory is that it was in the hundreds of thousands of pounds. The pirates and hackers were worked day and night to upgrade their cards with the new code. In bars throughout the UK, queues formed of eager customers, their beer in one hand and a pirate card in the other. The new code did not last long. Sky and News Datacom struck back with another ECM. This one was good. It was difficult for the hackers to solve.

The timing of the event had sown the seeds of uncertainty in the minds of pirates. Was it a sting by Sky? Was it a totally pirate operation? The full story has not yet been established. There was so much lying and deception going on that it was difficult to know who was involved.

What followed was a long hot summer of false starts and disgruntled customers. It seemed that Sky was winning as some of the pirates customers were signing up with Sky again but most decided to go with EuroCrypt-M cards and watch other channels. It was also possible to obtain a smart card from legal outlets and have it authorized for a few weeks. This ensured that those who wanted to view Sky were able to.

The Phoenix Program

The code auctioned in June made its way to the TV-CRYPT group where it was analyzed. The algorithm was an improvement on the 07 algorithm, but there was something else.

By rewriting the code it was possible to generate a correct checksum for any packet of data. By using a decoder emulation program it was possible to have an authorized smart card treat any data packet sent to it as valid.

This was a significant discovery. Sky's VideoCrypt system operated on an over the air authorisation procedure. Therefore if a data packet with a correct checksum was sent to a card it would be possible to switch on cards without the intervention of Sky. The card would not be able to tell the difference between a packet from a decoder emulator program and the real decoder.

By phoning Sky and having them turn on some legitimate cards over the air, it was possible to build up an understanding of how the authorisation scheme worked. The program was called Phoenix after the mythical bird. By the first week in August, the Phoenix program was posted.

To the TV-CRYPT the Phoenix program was an intellectual exercise to see how the VideoCrypt system worked. Some pirates saw things differently. They sold the program in some cases for thousands of pounds.

Genesis - Exodus - Exitus

The Star Trek influence runs through these hacks. Genesis was part of the plot of one of the Star Trek movies. One of the first commercial hacks was named Genesis. This was the combination of the Phoenix code and a blocker program. The combined program was loaded into a PIC16C84 microcontroller. One device could turn on all channels on a Sky card and block any kill signal that Sky sent to that card.

Sky had totally lost control of their access control system. Even the 09 issue cards that Sky had previously turned off were being reauthorized. The problem had gotten out of control. Sky and News Datacom were searching desperately for some solution.

It seemed that Sky, through their Quick Start scheme had supplied the pirates with all the genuine Sky cards that they needed. The going price for a QS card in September reached 60 pounds (about \$95). The legitimate dealers were getting them from Sky at 5 pounds per card (about \$8).

After what can be described as a war of attrition, News Datacom came up with an ECM that completely killed the cards activated by Genesis blockers. These dead cards could not be reauthorized. However September 1994 was a very bad month for Sky. From pirate sources, who were monitoring the over the air data, it became apparent that Sky were trying to kill every card that it could not account for. In that month alone, Sky killed 569430 cards. It is not clear how many of these were QS cards and how many were people just giving up watching the Sky channels. The October kill figure was 220073.

Legal Action In The UK

Sky eliminated its security department in March 1993 even though this internal group had succeeded in stemming the flow of piracy in the UK. It was a stupid decision for which they would pay dearly.

A deluge of ill-considered legal action followed in the UK. Sky prosecuted the "small guys" who did not have the money to defend themselves. These people were breaking the law in the UK but in prosecuting it was a public-relations nightmare. They created martyrs.

In one case Sky drew the media's attention by trying to claim that the defendant was a main dealer for Genesis blockers. However as the defendant had only 300 blockers, it was obvious that he was not a larger dealer.

In a Sky affidavit in the case it was estimated that Sky lost 2.25 million pounds to piracy between January 01 and May 18 1994. According to their estimates there 50,000 subscribers lost. According to Hack Watch News, there were about 300,000 pirate Sky cards in the UK at the beginning of the year.

The 09 issue of cards in February 1994 cost Sky approximately 21 million pounds. The next card issue, 0A, due in September 1995, will probably cost another 21 million pounds (\$30 Million).

Another card issue (0B) would be necessary in February 1995 if Sky wants to maintain the security of its system. The present annual cycle is not short enough to deter pirates. Sky originally planned to change the

cards every three to six months. This would provide the pirates with a moving target. When the company changed to a longer cycle hackers saw the system as a very big sitting duck.

The Cloning Of VideoCrypt

A sure sign that VideoCrypt was defeated was that it was cloned. The clone system, called KeyCrypt, was demonstrated at the London Cable and Satellite Show in April 1994. The company that had cloned it, Hi Tech Xtravision, had previously reverse-engineered a rather complex Application Specific Integrated Circuit (ASIC) as part of a hack on a digital audio system. They also had a far better idea for a customized smart card which would prove a lot more difficult to hack. A case perhaps of poacher turned gamekeeper.

Despite the potential benefits of KeyCrypt, broadcasters who want to use it can't. Some undecided copyright issues prevent them from doing so.

The Present Day

At the time of writing, VideoCrypt is still hacked. There are a few working Omigod programs available for the PC and the MAC that can hack all of the VideoCrypt channels. These programs are free - most of the BBSes in Europe have copies. When Sky implements an ECM, the modified versions of the programs are posted on the BBSes within a few hours - an embarrassing situation for News Datacom and Sky.

Many of the pirate smart cards on the market now use American technology. One card has a keypad. When there is an ECM, the pirate card user just telephones an answering service to retrieve set of numbers. He then enters the numbers on the keypad and the pirate card resumes operation. Another card uses a modem. So when there is an ECM the modem does all of the hard work.

Things will change over the next few months though if Sky brings out its new OA card. Then the pirates may be defeated - for a while. However, the problem is that nobody is sure how long the new card will remain unhacked. The most important lesson that the DSS broadcasters could glean from the European experience is that the cards have to be changed every six months. Otherwise it is certain that they will be hacked.

[Return to main page](#)

Copyright (c) 1995 Hack Watch News

Re: [NOISE] Cable-TV-Piracy-Punks

Hack Watch News (kooltek@iol.ie)
Fri, 29 Mar 1996 20:53:18 +0000

- Messages sorted by: [date] [thread] [subject] [author]
- Next message: Duncan Frissell: "Account ID Controls"
- Previous message: Black Unicorn: "Note: Problems Confronting the Asset Concealer [Part 1 of 2 of Volume I]"
- Next in thread: Mike Duvos: "Re: [NOISE] Cable-TV-Piracy-Punks"

> "David K. Merriman" <merriman@arn.net> writes:

>
>> At 01:34 AM 03/28/96 +0000, you wrote:
>
>>> I've been looking for a file on how to make PPV
>>> descramblers and haven't found any. Commercial descramblers
>>> cost around \$200 base price. If anyone has a file on how to
>>> make them please e-mail me one. Thanks.
>
>> This is cypherpunks. Not Cable-TV-Piracy-Punks.
>
> ObCrypto: Scrambling TV signals sometimes makes use of
> encryption, so perhaps a brief discussion of how this is done
> could be tolerated.
>
> If you are talking about recovering signals from completely
> encrypted digital MPEG-2 streams, such as those used by the DBS
> folks, you are probably out of luck. The relevant processing in
> the decoder exists on a small card which has so far resisted
> attempts at reverse engineering.
>

The DSS smart card has been reverse-engineered for at least six months now and pirate devices are in the market. The encryption used on those systems is good but it does not stand up to a well financed attack. In the European version of the system, the encryption routines were using a hashing function. The input packet also carried the authorisation data so it was using this as an input packet. The DSS routine is probably based on a similar hashing routine.

> There are a variety of techniques for scrambling audio. The most
> expensive is to DES encrypt the sound and place it in the
> horizontal blanking interval. The regular sound channel can then
> be used for advertising. This requires a bit of processing at
> both ends, and is generally used for satellite to ground
> transmission of cable signals. The other common method is to
> modulate the sound on a subcarrier, usually the one transmitted
> in phase with the missing sync.
>

Using DES to encrypt the audio on the fly is an old technique and was used in the VideoCipher II system. Most of the more recent systems use a PRNBSG EXORed with the digital audio data stream.

>Of course, once television transmission goes completely digital,
>and strong encryption is used on both audio and video, the
>opportunity for such simple attacks will vanish.
>

The problem of piracy will still exist on digital systems. The DSS system is a completely digital system and it too is hacked. Admittedly some of the elements of security in the DSS are good, most can be rendered void by hackers. The problem for DSS is that the smart card they used is not secure enough. It was a Motorola 6805 type. What appears to be the pattern with the hacks on more recent smart card systems is an inversion of the original pattern on the simple analogue systems. The original pattern was that some hobbyists would figure out how to hack the system and then the hack would be commercialised. With the smart card hacks - the pattern is inverted so that it becomes a trickle down pattern. The professional hackers reverse and emulate the smart card and then the code is sometimes hacked from the emulator card and then distributed among hobbyists.

The most dangerous thing in all this is that the smart cards that have been hacked in Pay TV systems throughout the world are also used in other applications. The expertise and the knowledge of reversing smart cards is now more common in the Pay TV piracy business. There is always the possibility that these skills could be applied elsewhere.

Regards...jmcc

John McCormac * Hack Watch News
jmcc@hackwatch.com * 22 Viewmount,
Voice&Fax: +353-51-73640 * Waterford,
BBS: +353-51-50143 * Ireland

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6

```
mQCNAzAYPNsAAAEEAPGTHaNyitUTNAwF8BU6mF5PcbLQXdeuHf3xT6UOL+/Od+z+
ZOCAX8Ka9LJBjuQYw8hlqvTV5kceLlrP2HPqmk7YPOw1fQWlpTJof+ZMCxEVd1Qz
TRet2vS/kiRQRyVkoAxoJhqIzUr1g3ovBnIdpKeo4KKULz9XKuxCgZsuLkVAAUX
tCJkb2huIE1jQ29ybWFjIDxqbWNjQGhhY2t3YXRjaC5jb20+tBJqbWNjQGhhY2t3
YXRjaC5jb20=
```

=sTfy

-----END PGP PUBLIC KEY BLOCK-----

- **Next message:** [Duncan Frissell: "Account ID Controls"](#)
- **Previous message:** [Black Unicorn: "Note: Problems Confronting the Asset Concealer \[Part 1 of 2 of Volume I\]"](#)
- **Next in thread:** [Mike Duvos: "Re: \[NOISE\] Cable-TV-Piracy-Punks"](#)