PMK

May 19. Version after many comments on May 18

(4 typos given to Ron via voice mail May 22).

DIRECTV PROPRIETARY II

DIRECTV

NDS

DIRECTV and NDS Card History and Technical Discussion

Ron Cocchi
Perry Smith

Version 1.0

DRAFT

DIRECTV PROPRIETARY II

CASE NO.
SA CV 03-950 DOC (JTLx)
ECHOSTAR SATELLITE CORP., et al.,

vs.

NDS GROUP PLC, et al.

DEFENDANT'S EXHIBIT 391

DATE ________________ IDEN.

DATE ________________ EVID.

BY____________________
Deputy Clerk

PMK

May 19 Version after many comments on May 18

(4 typos given to Ron via voice mail May 22.)

DIRECTV PROPRIETARY II

DIRECTV

NDS

DIRECTV and NDS Card History and Technical Discussion

Ron Cocchi
Perry Smith

Version 1.0

DRAFT

DIRECTV PROPRIETARY II

Kahn
EXHIBIT NO. 39
6/6/07
D.JANNIERE CSR#10034

DIRECTV and NDS Card History and Technical Discussion
DRAFT

Table of Contents

1 Introduction 1
2 Meeting History 2
3 Actions 2
4 Documents 2
5 Card Heritage 3
5.1 Card Comparison 3
5.2 Analog verses Digital Systems 6
5.3 NDS Software Review 7
5.4 Technical Risks Delaying P3 Card Change 8
5.5 IRD Manufacturer and Mailout Cards 9
5.6 More on Cards 11
6 Card Technical Details 13
6.1 Internal Analysis 14
6.2 Internal Probing Attacks 16
6.3 Hardware Components 17
6.4 Optical ROM Code analysis 19
6.5 External Analysis 19
6.6 Primary Attack Scenarios 22
6.7 Strong and Weak Aspects 24
6.8 Defenses Not Uncovered 24
7 Security and Cryptography Research Relationship 27
8 Summary 28

DIRECTV and NDS Card History and Technical Discussion
DRAFT

1 Introduction

This document was written to review the security and integrity of the P3 card. The objective of developing and deploying a new card is to eliminate piracy. An extremely secure card should be very difficult to break. After a sufficiently long period of time without breaking the card, the hacker tends to move to other targets that are perceived as being more vulnerable.

This report is the result of a series of technical discussions between DIRECTV and News Digital Systems (NDS). The purposes of the discussions were to educate DIRECTV in two areas critical to the security and integrity of its direct to home pay television business and to ensure that DIRECTV has the highest possible security in its new card.

The first area of discussion relates to the heritage of the Conditional Access Module (CAM). A CAM is the access card that resides in every subscriber's set top box. It is one of the most critical components in maintaining security for DIRECTV. It is important for DIRECTV to understand the technical decisions that were made in previous access cards and to inquire how they can be made more secure in the future. In understanding the heritage, DIRECTV is most interested in the technical similarities that exist between its card and those of other systems developed by NDS used by their other customers.

The second area of discussion relates to understanding the security mechanisms utilized by the Period 3 (P3) access card. The two previous cards, P1 and P2, were broken by a very educated and resourceful hacker community. The P2 card was broken before it was completely deployed. NDS has taken considerable measures to ensure that the P3 card is far superior to any card it has fielded for commercial use. NDS has contracted with TNO to review the security and integrity of the hardware aspects of the card. The details of this report will be discussed in this document. NDS has also implemented its own software review process. DIRECTV is currently having Cryptography Research (CR) perform a black box evaluation of the P3 card. CR is a firm that specializes in system attacks as opposed to hardware invasive attacks utilized by TNO.

DIRECTV discussed the new openness in the relationship with other Hughes Electronics Direct Broadcast ventures, namely Galaxy Latin America (GLA) and DIRECTV Japan (DTVJ). Conditional Access is one of the areas where technical discussions have occurred. In the case of GLA, the communication is bi-directional and has been beneficial to both organizations.

Authorized participants in creating and reviewing this document are Ron Cocchi, Ray Kahn, Peter Klaus, Yossi Tsuria and Perry Smith.

2 Meeting History

Objective	Location and Date	Attendees
Card Heritage and Technology	London, 17 – 18 Mar 99	Ron Cocchi, Ray Kahn, Yossi Tsuria, Perry Smith
Card Technology Follow up	New York, 18-19 May 99	Ron Cocchi, Ray Kahn, Peter Klauss, Perry Smith

3 Actions

Num	Action	Respondent	Due Date	Date Comp
1	*Create first draft of Card History and Tech Discussion Document*	Ron Cocchi	24 Mar 99	1 April 99
2	Create rebuttal to key issues raised in the TNO report	Perry Smith	21 April 99	
3	Deliver Hierarchical Key White Paper	Yossi Tsuria	1 April 99	1 April 99
4	DPA paper from Cambridge	Yossi Tsuria	1 April 99	
5	Revisit areas where illegal jump instructions may be executed, caused by descrambled FFh reads subject to illegal voltage levels	Perry Smith	15 May 99	
6	Review NDS System Attack Doc	Ron Cocchi	Jun Qrtly?	
7	Determine who has the P4 prototype	Ron Cocchi	14 April	
8	Consider setting up a meeting between Adi and Paul to discuss key distribution	DIRECTV	21 April	

4 Documents

The following document were reviewed and summarized when creating this report.

1. *DIRECTV – NDS P3 Security Meeting,* PowerPoint presentation, written by Perry Smith, March 1999.
2. *Evaluation of the physical security aspects of the Shepherd chip*, document number EIB-RPT 980035, written by TNO, 17 April 1999.
3. *Evaluation of the physical security aspects of the Shepherd chip: Summary report*, document number EIB-RPT 980045, written by TNO, 13 July 1999.

5 Card Heritage

The initial card change out philosophy use in the British Sky Broadcasting (BSkyB) was to change out cards every three months. This philosophy was in place to continuously stay ahead of hacker attacks. It was quickly realized that this approach was not operationally feasible. The change out duration was lengthened to 6 months then to 12 months and eventually longer.

5.1 Card Comparison

Figure 4.1 shows the relationship between DIRECTV, BSkyB, GLA and DTVJ cards.

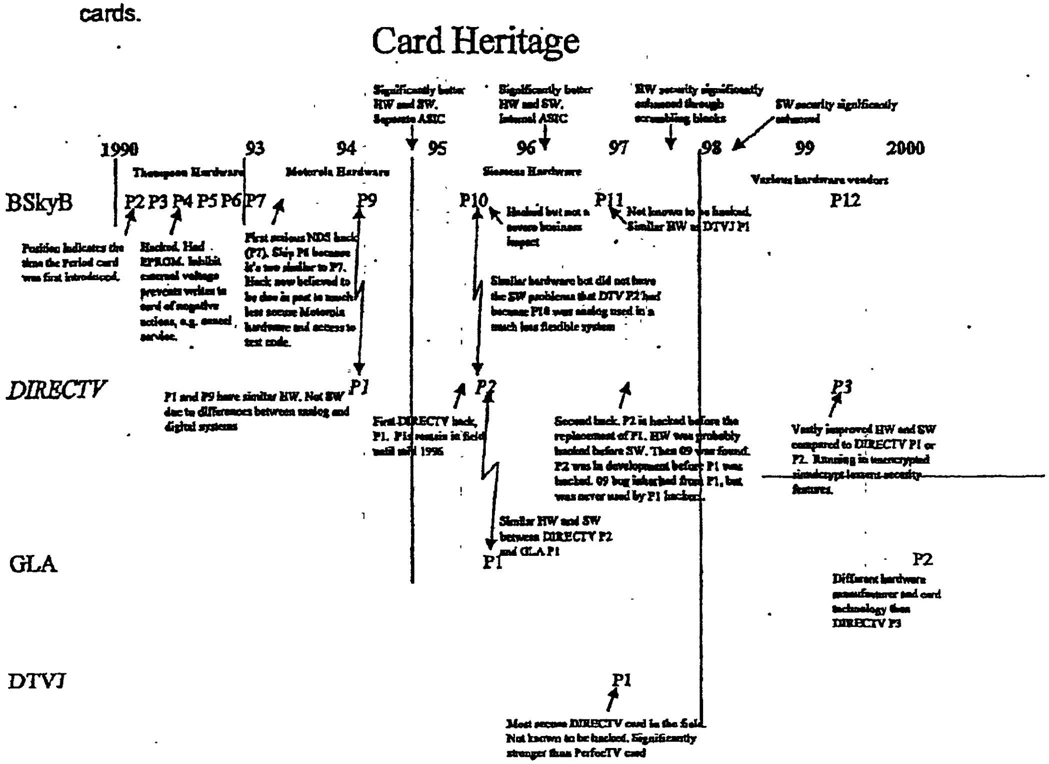
Card Heritage
Significantly better HW and SW. Separate ASIC
Significantly better HW and SW. Internal ASIC
HW security significantly enhanced through scrambling blocks
SW security significantly enhanced
1990
93
94
95
96
97
98
99
2000
Thompson Hardware
Motorola Hardware
Siemens Hardware
Various hardware vendors
BSkyB
P2 P3 P4 P5 P6 P7
P9
P10
P11
P12
Position indicates the time the Period card was first introduced.
Hacked. Had EPROM. Inhibit external voltage prevents writes to card of negative actions, e.g. cancel service.
First serious NDS hack (P7). Skip P8 because it's too similar to P7. Hack now believed to be due in part to much less secure Motorola hardware and access to test mode.
Hacked but not a severe business impact
Not known to be hacked. Similar HW as DTVJ P1
Similar hardware but did not have the SW problems that DTV P2 had because P10 was analog used in a much less flexible system
DIRECTV
P1
P2
P3
P1 and P9 have similar HW. Not SW due to differences between analog and digital systems
First DIRECTV hack, P1. P1s remain in field until mid 1996
Second hack. P2 is hacked before the replacement of P1. HW was probably hacked before SW. Then 09 was found. P2 was in development before P1 was hacked. 09 bug inherited from P1, but was never used by P1 hackers.
Vastly improved HW and SW compared to DIRECTV P1 or P2. Running in unencrypted simulcrypt lenient security features.
Similar HW and SW between DIRECTV P2 and GLA P1
GLA
P1
P2
Different hardware manufacturer and card technology than DIRECTV P3
DTVJ
P1
Most secure DIRECTV card in the field. Not known to be hacked. Significantly stronger than PerfecTV card

Figure 4.1

DIRECTV and NDS Card History and Technical Discussion
DRAFT

The table below shows technical relationships among Period cards of NDS DTH vendors.

Sys / Period	HW Vendor	Memory	Hacked	Comparison
BSkyB P1-P4	Thompson	2K ROM, 1K EPROM, 44B RAM	No	Sky P2 – P6 designed for 3 month change out. Change out interval was increased to 6m, 12m then 18m due to increasing sub counts and logistics
BSkyB P4-P6	Thompson	2K ROM, 1K EPROM, 44B RAM	No	EPROM had external program voltage. Had trouble with valid writes. (Hackers blocked the EPROM write voltage) Attack not widely exploited.
BSkyB P7	Motorola	3K ROM, 1K EEPROM, 128B RAM	Yes	First serious NDS hack. P8 skipped because it was too similar to P7. Motorola made a few HW changes in making the card. NDS wanted more HW changes Urban legend that ex-Motorola employee revealed special test code.
BSkyB P9	Motorola	6K ROM, 3K EEPROM, 128B RAM	Yes	Foundation for DIRECTV P1. Similar HW
BSkyB P10	Siemens	8K ROM, 4K EEPROM, 256B RAM	Yes	Basis for DIRECTV P2 card. Had asymmetric signature, unlike P2. Did not have software problems of P2 because it was an analog system with a well defined and fixed feature set, i.e. not designed to be flexible. PC conn hacked asymmetric signature
BSkyB P11	Siemens	8K ROM, 4K EEPROM, 256B RAM	No	Still not known to be hacked. Similar to DTVJ P1. One chip integrated ASIC solution.
DIRECTV P1	Motorola	6K ROM, 3K EEPROM, 128B RAM	Yes	SW designed for business flexibility and extensive features squeezed into small code space. System was hacked when DIRECTV approached 2 million subs. Initial hacks used Motorola HW holes. SW protocol attacks using invalid msg structures caused stack overflows that allowed access into SW. Also had 09 hole that was inherited by P2, but not used in P1 hacks. Card was taken from Sky P9. Motorola made HW changes for DIRECTV P1 unlike in Sky P7. Less than 5% similar SW to Sky P9, no EMM, new BIOS, different baud rate.
DIRECTV P2	Siemens	8K ROM, 4K EEPROM, 256 RAM	Yes	Designed to be flexible. Derived from Sky P10. Had symmetric, 5 byte signature. Has an external ASIC. DIRECTV P1 and P2 cards are 70-80% similar excluding assembly language differences due to separate HW manufacturers.. DIRECTV P2 and GLA P1 are 70-80% similar. Differences are in features and security routines. Few new feature bugs in P2 vs. P1. There were more code bugs. Known stack problems in P1, fixed in P2. 09 hole first used in DIRECTV P2 hacks, then found in P1 and in GLA P1.
DIRECTV P3	Texas Instrmts	16K ROM, 8K EEPROM 384 RAM	N/A	TI chosen because of flexibility. Hardware vendor agreed to design a unique card. One chip integrated ASIC solution. Half of EEPROM is data. 50-70% similar to DIRECTV P2 before making the code more secure. 0-10% after code was made more secure. Has asymmetric 8 byte signature. First card on which NDS had an extensive internal SW review
GLA P1	Siemens	8K ROM, 4K EEPROM, 256B RAM	Yes	09 hole. Very similar to DIRECTV P2. see above.

GLA P2	Siemens	25K ROM, 16KEEPROM 512B RAM	N/A	
DTVJ P1	Siemens	16K ROM, 8K EEPROM 256 RAM	No	Strongest card fielded in any DIRECTV system, excluding DIRECTV P3.

Ask Perry for code similarity between DTV P3 and GLA P2. Code shared. Technical differences? Hardware differences?

Ask Perry for code similarity between DTV P3 and SKY P12. Code shared. Technical differences? Hardware differences?

P1 hacks were first discovered in November 1995. P2 cards were first sent to IRD manufacturers and sent out in boxes in July 1996. The P1 algorithm was turned off in July 1997. The first P2 hack was discovered in July 1997.

Little was known about how the system would evolve and how operations would take shape. As a consequence, P1 and P2 cards were designed to give maximum flexibility while the system evolved. Allowing flexibility lead to the introduction to the 09 hole. Squeezing in functional features into limited code space meant less room for carefully counteracting out-of-spec inputs. The P2 card was hacked and the code available on the Internet. The P2 algorithm cannot be replaced because the hacker community will receive the download and understand the changes.

The DIRECTV P3 card architecture is significantly different than previous generations of DIRECTV and NDS cards. It is the only NDS card produced by TI and has different operational codes (opcodes). Opcodes of the TI chip were modified to create a truly unique operating environment for the P3 card. New instructions were created and others were renumbered. This process hides the native functionality of the processor and makes it harder to reverse engineer the code. *An off the shelf TI processor emulator cannot be used.*

NDS chose TI because they were an unknown manufacturer to the smart card business who wanted to enter the market. TI worked closely with NDS to build a unique and secure chip. TI committed to making custom modifications to the chip.

P3 features several security techniques not included in previous cards. The *techniques used in P3 are far superior to those used in prior cards.* These measures make it extremely difficult to reverse engineer the logic. The following provides a summary of these techniques. Security measures and techniques will be discussed in detail later in this document.

1. Circuit camouflage: includes hiding logic gates to trick uneducated observers into thinking that gates perform other functions

2. Five levels of encryption: includes encrypting actions in packets, packets, data in the card, and HW encryption
3. More flexible DDT mechanism: DDT has more actions. Can combine actions. In P3, one packet/action is sent for the population (could be to general population) and other packets/actions are built upon it (group addressed or to limited population). Can generally sign packets instead of group addressed for some actions. The effect is to send fewer packets, closer together. In P2 DDT packets are sent to groups of 256 subs, creating 30,000 packets to cycle through before any single subscriber receives a retransmission.
4. More flexible software download mechanism: P2 was internally limited to 8 bytes per write action and download capability to two locations (4 bytes in one location and 4 bytes in another location). A P2 download increased this value limited to the packet size. The download mechanism in P3 is more general. P3 can send more data and to more locations. Can set the length of the download action and not limit it to 4 bytes. Download in P3 is more flexible and not limited to group addresses.

It is not agreed within NDS whether, in hindsight, TI was the best choice. TI offered the best security in comparison to what was available by other vendors at the time, but others have caught up. TI has not manufactured chips for any other NDS project and may not be selected for P4. However, P3 has undergone significantly more review than any other NDS card and has the advantage of being very different from every other smart card on the market. This P3 architecture makes it difficult for a hacker to learn about the technical details of an unknown chip.

NDS started using 50-70% of the P2 code, converted it to the TI instruction set, then made the code more secure. When John Markey was hired to head the Conditional Access department, he requested that the entire P3 coding effort be restarted to pay much more attention to the possibility of software-based hacks and protocol misuse. After the rewrite, less than 10% of P2 code remained in P3. With more new code there is always the risk of introducing more new bugs.

5.2 Analog verses Digital Systems

BSkyB is largely an analog system. Its cards were used as the basis for the DIRECTV period cards. Sky P7 and P9 cards were the basis for DIRECTV P1. Sky P10 and DIRECTV P1 cards served as the basis for DIRECTV P2. While Sky P9 and P10 were hacked, NDS reports they were not subject to protocol hacks as the DIRECTV cards because analog systems are very simple and offer little flexibility within their fixed structure. These systems are usually synchronous. DIRECTV was the first high power DTH system with a very flexible messaging command structure.

A BSkyB 32 byte analog packet has the following fixed structure. The system is synchronous and hence has no header or length.

Byte 1: Control Byte for packet type
Byte 2: Month
Byte 3: Data byte used for flags
Bytes 4 and 5: Either random for service or contains PPV number for PPV
Byte 6: Channel and Rating (similar to DIRECTV 2 byte service id). DIRECTV has no channel byte to the card.
Byte 7: Action. Enable or disable channel or OSD number
Bytes 8 – 26: Addressing
Bytes 27 – 31: Signature
Byte 32: Checksum

5.3 NDS Software Review

Writing code for a smart card application is unlike writing code for other applications. The card and software within the card are subject many external attacks which are difficult to plan for or anticipate. The card may be subject to clock speed up, clock slow down, voltage change, and manipulating instruction execution sequence.

The DIRECTV P3 card is the first card for which NDS conducted an extensive software review. DIRECTV made a technical decision to delay deployment of the P3 card so that the software security of the card could be reviewed. Hence NDS was able to allocate a staff to conduct an audit of the software.

NDS developed the P3 card over a three-year period. Three people developed the hardware over a period of two years (6 man-years). Two people wrote the functional aspects of the software over an 18 month period (3 man-years). The software review to make the code secure required an 18 month period: 6 reviewers over 4 months; 3.5 reviewers over 5 months; and currently 1.5 reviewers over 5 months (4 man-years).

The reviewers came from both within the NDS security department as well as from other parts of the company. NDS has developed a document containing all known attacks of both HW and SW. Yossi will allow DIRECTV personnel to view the 1.5 inch thick document next time they are in Israel.

As a result of the software review process, the P3 card is the first to have major structural improvements to the code. In P1 and P2 NDS focused on making the code operate as expected and did not extensively test conditions outside the boundary conditions of input message, structures and protocol. This was due primarily to their emphasis being placed on the security of the hardware. They believed it would be very difficult to read the code off the card in order to learn the boundary conditions. NDS claims they had never encountered these types of hacks in their analog system.

The P3 code is written to protect against input boundary conditions. The code flow is also designed to be secure even when instruction skips are induced by illegal voltage and timing variations.

TNO reported that manipulation of the power supply voltage during a read cycle from ROM or EEPROM could return fetch opcode of data to have all ones on the data bus, (FF). When descrambled this could result in an illegal jump instruction or other unintended action. NDS has agreed to revisit areas where illegal jump instructions may be executed.

5.4 Technical Risks Delaying P3 Card Change

Clearly a preliminary analysis from Cryptography Research (CR) needs to be evaluated before any decision to mail the P3 card is made. Their analysis should be completed prior to the May P3 meeting with NDS. Given that TNO was *not* able to break P3 despite their claim that they have been able to break every other card they analyzed and assuming that the CR report is favorable, there would be no technical reason to delay the card change.

Further, delaying the P3 card change jeopardizes the future security and integrity of the P3 card. P3 accepts the encrypted CAP stream and CWPs. Simulcrypt does not allow encrypted CWPs while P2 cards are in the field. Delaying the card change creates a period of time in which the P3 is more vulnerable to attack until the P2 algorithm is turned off and the CWPs are encrypted. Much can be gained through examining the packet stream and downloads. Paul Kocher from CR was able to learn a great deal of information about the GLA system through examining the software downloads. The inputs of P2 are well understood and information obtained when simulcrypt is present can be used to compromise the future security of P3.

Also the hardware security of P3 was developed in 1996 for deployment in late 1997. Card technology has advanced significantly in the past two years (0.35 µm vs. 0.7 µm in 1997), while P2 has been in the field for the past 4 years. A new P4 card cannot be developed and fielded in a timely fashion that would eliminate the requirement to field a P3 card. The longer the delays in fielding P3 the less secure that solution becomes. Yossi believes that under ideal circumstances it will take 12 months for hacker hardware reverse engineering of P3. He believes that it will take much longer for the hacker to produce a commercialized reverse engineered private card for sale, i.e. to develop a green card with an ASIC.

Ultimately how long P2 remains in the field affects the hackers ability to stay in business and how fast they will pursue easier targets. Slowly rolling out P3, extends the life of current hacker resources. An example is Sky P11 card that NDS reports has not been hacked for 25 months. NDS reports that all European cards have been hacked and that hackers have moved away from P11 to get to other European Systems provided by vendors such as Irdeto, Nagra, etc..

5.5 IRD Manufacturer and Mailout Cards

The first cards received by hackers come from IRD manufacturers. Much has been done over the last few years to limit the unauthorized distribution of access cards. But the fact remains that this problem is very difficult to control because the economics are difficult to combat in the third world where the IRD manufacturer factories reside. Low wage workers may be offered a year's salary for 5 thousand access cards.

NDS designed a mechanism that would make cards received from manufacturers harder for a hacker to break and convert into an unauthorized access card. The concept involved leaving out key information from the access card delivered to the IRD manufacturer. This data would be sent to the subscriber as part of the activation. The missing data is that required to generate a valid Control Word (CW) and is implemented by filling a table with random, invalid data instead of the data required to generate a CW. This field is 12 bytes and used in the hashing function to generate a control word. The information is related to the asymmetric algorithm stored in the card. This information is required to generate a valid signature but is not required to validate a signature in a packet. The information is sent to all cards, i.e. not just to D cards,

Cards sent to subscribers are required to implement *chaining*, a procedure to copy the PPV and key information from an old card to the new card. Immediately after chaining it is necessary to generate a valid CW. Chaining occurs without input from the headend. Therefore, the mailing cards must be manufactured with the correct data table. The cards created for IRD manufacturing will not function properly if mailed to an existing subscriber who requires chaining.

Making the card requires it to be processed by the manufacturer line twice. During the first production pass the image is loaded on the card. In this stage the table is loaded into *M* cards. During the second pass the CAM number is imprinted on the card.

The following table lists the current P3 cards

Card	Description
3.0D	IRD Manufacturer card. Functional in all IRDs except HNS B boxes.
3.1D	IRD Manufacturer card. NDS removed the inverter on the clock. HNS B relies on the rising

	edge of the Input clock.
3.1M	Mailing card. Contains data necessary for generating the CW required immediately after chaining. Same hardware as 3.1D.
3.2M	Mailing card. needed to prevent card failures durin brief power outages for HNS A box. Holds reset when Vcc is low. Metal layer fix to the card. May cause the card to be less reliable.

NDS used TI and their design engineers to build the multiple versions of chips required for P3.1 and P3.2 cards. It is unlikely that this level of cooperation would have been accomplished with other hardware suppliers.

The P3.2 card is physically different than the other cards and will be supplied only to the owners of HNS A boxes. A metal layer fix was applied to the card. The HNS A box failed to hold reset low until Vcc was fully high. This action allowed the card to start operation at an improper Vcc, which caused the card to self-destruct. The self-destruction of P3 under improper voltage level operation was not an intentional design feature, but does serve as a protection against pirates who attempt to extract information by operating the card at improper voltage. The P3.2 metal layer fix holds the reset low for a fixed number of clock cycles after Vcc starts to be applied. This protects against card failures in HNS A boxes. But this makes it easier for hackers to vary voltage levels when trying to hack the card. Therefore, P3.2 is more susceptible to attacks using Vcc out of range voltage levels. Knowledge gained from these attacks can be used to break other cards that are protected when voltage levels are outside defined thresholds. Other P3.x cards will self-destruct when intermediate voltage levels are outside defined bounds. This lack of protection is not perceived as a great threat because P3.2 cards will enter operations late in the replacement cycle and only approximately 600,000 will be produced (estimated 300,000 to 400,000 IRDs in the field). Most HNS A box are owned by long time, loyal DIRECTV subscribers. There is nothing on the card to indicate that the card is physically different. There are unique marking to identify the various P3 cards. The markings could ease an attacker in breaking the card if they cal learn how to capitalize these differences.
Ask Peter for the encodings and for details on the software differences in the versions. Only the CAM ID range, which is not unusual, identifies the card type.

In later model IRDs, HNS did not use the Thompson transport chip but designed their own. Since the software did not change, HNS decided not to do integration testing with NDS. This decision lead to the HNS-P3 problems. The drivers behind moving away from the Thompson chip were the license fee, poor documentation and HNS's preference to make their own highly integrated chips.

The original design for the Sony 4th generation box would not operate properly with the P3 card. It has flow control problems occurring at 11.4 ETUs as listed in the specification but in operations the timing can be less precise. Six months ago, NDS cleaned up the specification in this regard by explaining the interpretation of the timing table. NDS offered to reimburse Sony for some of the nonrecurring engineering and will allow Sony's box to enter at the head of the testing queue. There are three likely solutions:

1. Change Sony TI transport chips. NDS reports a first attempt to modify the chip was not successful. If a second attempt is successful, this approach will most likely lead to the quickest resolution.
2. Change Sony software. NDS reports that this approach will require a board change and if so this approach will likely delay Sony's planned launch date.
3. Change smart card software. Invalidates DIRECTV's testing effort and introduces another card.

Sony elected choice 1.

The ultimate hack is one where no NDS card is required. That is, the hacker develops a solution that requires no NDS hardware to gain access to the DIRECTV pay services. One successful hack of the P1 involved creating a green circuit card that fit into the access card slot with an extension that came out of the IRD. In P2, all communication to the CPU goes through the ASIC. See Figure 4.5.1. Early P2 pirate websites also suggested the possibility of drilling into a P2 card and intercepting the flow between CPU chip and card ASIC chip. An early P2 rumor that has recently resurfaced on the Internet was that the hacker industry was able to either pull out the ASIC of a P2 card or manufacture an ASIC and place it on the green circuit card. NDS has substantiated this rumor and now believes that a P2 hack has been achieved by removing an ASIC from a P2 card and placing it on a green card (NY Meeting 18 May 1999). Commercial viability is not known to be successful at this time. The approach is complex and expensive to achieve. No evidence exists to indicate that the ASIC has been reverse engineered and commercially produced. In contrast a blue card hack is one where the card looks like an existing card and fits completely into the IRD.

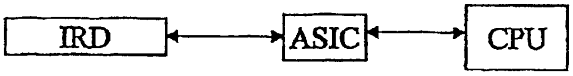

Figure 4.5.1 IRD communication

5.6 More on Cards

Sanctions: A card whose operations are considered outside normal boundaries may implement sanctions. The card can either turn off service or self-destruct depending on the severity of the infraction. NDS believes that self-destruct is too severe for many circumstances. For example, it would not be prudent to kill a card just because of bad signature verification. In this case a bad signature sent by DIRECTV could cause a significant portion of valid cards to blowup. NDS believes that putting in a counter to track these conditions would be more flexible and effective. An ECM could be sent at a later time to kill cards with a counter that exceeds some predefined threshold. This approach may differ from a Visa application that has a 1:1 connection to a financial clearinghouse. PAY-TV has a 1:many relationship and must be more careful in how to implement countermeasures.

Echostar hack: The current Echostar card uses a Thompson ST16 chip. The hack, discovered 3-4 months ago, affects *all* Nagra installations. The card has been in operations for 3+ years. The hack requires a modification to the IRD performed by the *subscriber* or third party supplier. The solution can be obtained over the Internet.

The Nagra card allows an external interrupt to be generated, because that use RSA public key operations, which are time consuming. In order to process an ECM (DVB encryption control message, similar to our CWP, which carries the new CW), they issue an interrupt to the RSA process in the card. NDS does not allow external interrupts because it is risky. The Nagra card has a socket bug where interrupts are not disabled during the card startup routine. This action allows an attacker to generate an external interrupt before the internal registers are setup correctly and hence gain illegal access to the code.

The fault exists before access to EEPROM, so it can't be fixed by an EEPROM software download. An attacker interrupt routine allows a subroutine to read in bytes and take control of the card in a similar manner as NDS's stack overflow problem. The problem can be fixed by a card change. Nagra has never done a card change before. Not doing a card change has been a marketing feature for Nagra. To fix the problem, Nagra must disable and enable interrupts correctly. The card lasted for 3+ years because DIRECTV was so widely hacked and Echostar was not seen as a target due to their smaller subscriber base.

6 Card Technical Details

John Markey selected TNO because of their experience with breaking and assessing the hardware security of smart cards. NDS agreed with their credentials. TNO's areas of competency are in hardware evaluation and invasive attack methods.. NDS asked TNO to address the following three areas: 1) Evaluate the Built in system test software 2) attack chip by external evaluation methods and 3) attack chip by internal evaluation methods.

TNO was able to gain a great deal of information about the P3 card. NDS reports that most of the information in the TNO review is factual. TNO claims to have been able to break every other card they have analyzed in the past. They were not however successful in breaking the P3 card.

NDS has indicated that although TNO was able to learn much of the techniques of the card, there were significant counter measures that were not discovered during their evaluation. Many of these techniques will be addressed throughout this section of the report.

The TNO evaluation was to be a one-month effort conducted by between one and two employees. The evaluation began in Dec 97 and concluded in March 98 for a total of four months and consumed four employees. NDS paid 300K Guilders, approximately 160K USD, for the effort. TNO delivered a detailed report, EIB-RPT-980035, and later produced an executive summary version, EIB-RPT-980045.

In the report, TNO indicates techniques that were successful and others that were not and suggests additional attacks if NDS had more hardware development time. TNO points out strengths and potential weaknesses. They do not make any proposals or recommendations. It is TNO policy not to suggest methods to improve security, since they are concerned this will result in a flow of IP between different systems they examine.

Having the TNO report made NDS know where they stood in the world and what was hard for a lab to do and what was easy. TNO is extremely competent in this regard. They are better at this form of analysis than the hacker community. The techniques that TNO used require diverse disciplines. No one hacker group possesses enough knowledge to perform it. To counteract these complications, a hacker would contract out the difficult steps and perform the analysis in house. NDS intentionally designed the multiple security features in P3 with this goal.

NDS utilized the services of the TI branch in France. The TI development took longer than expected. At times TI appeared to be ~~fead~~ Fed up with NDS.

Consider writing an intro paragraph to the analysis *negative DDTs, positive DDTs notes page 4*

6.1 Internal Analysis

TNO examined the P3 card using a combination of invasive and analytical techniques including: exposing the die, topological analysis, chip information, bond pads, and wet etching. Each technique will be discussed in turn.

Exposing the die: The chip was exposed using chemicals to remove the module from the card and evaporate the epoxy resin off the module. NDS spent resources investigating secure packaging but could not find one that met a significantly higher standard while not introducing reliability issues and manufacturing complications. Later NDS felt that these issues could have been sufficiently addressed. Although it would have increased production costs, in retrospect NDS felt it may have been worth using. TNO experienced some difficulty in removing the resin since the resin that was used was standard but not common. TNO indicated that the resin came off in an unexpected manner. It came off in chunks instead of like a smooth paste.

The die was found to be significantly larger than expected. It measured approximately 27mm. Typically the dies range between 15 and 20mm. This caused complications for TNO in that their equipment was tooled for smaller sized hardware. NDS expected TNO's analysis to reveal more about the chip.

Topological analysis: TNO used microscopic examination to determine the positions of the main building blocks of the chip. This information was used to attack the most vulnerable areas. TNO was successful in locating the main building blocks such as I/O circuits, ROM, RAM, EEPROM, charge pump and processor core. TNO also discovered nonstandard components such as scrambling blocks and an unknown module that turned out to be the internal ASIC (discussed in more detail latter). The scrambling blocks were almost completely reverse engineered, much to the surprise of NDS. However, they did not discover that the scrambling blocks require additional steps before the data is useful. Also ROM is protected by an encryption function that was not discovered.

Of these components the ROM and EEPROM were custom components. The RAM was not customized.

Chip information: NDS revealed the processor type to TNO, although it's expected an attacker will have trouble determining the manufacturer. TNO confirmed that this information would have been difficult to extract from the chip. There are no manufacturer identifiers. It is hard to assess how secret this information is now.

The processor is a custom product with a TI TMS370 processor core. NDS scrambled the operation codes so that knowing the standard instruction set would not significantly aid an attacker. This makes disassembling the software much harder because a standard decompiler for the TI chip would not be of direct use.

There are no manufacturer identifiers. The names TI or TMS370 were not found. The only marking are building block identifiers (memory version numbers that NDS did not expect to have printed on) and the processor that had a stamp of *FINNLAND* across the top, which was placed by NDS to identify the chip type and confuse an attacker. Removing the building block identifiers would have required redoing the smart card mask. Removing as much of the marking as was done complicates the manufacturing process that frequently relies on the markings for calibrating the position of the chip.

Bond pads: Bond pads are used in part for testing the proper operation of the chip during the manufacturing process. Every chip is tested and hence contains bond pads. TNO identified thirteen bond pads on the P3, of which six are used for external connections. All pads had scratch marks from needles. Bond pads are commonly interrogated in order to find those used to enter test mode. If these are found, then they may be susceptible to exploitation yielding information that could lead to full external control of the chip. TNO expected to find SCANPASS, which might allow them to enter test mode and possibly reverse engineer the chip. They were *not* successful. NDS had this removed after much discussion with and resistance from TI. TI claimed that it would interfere with their fabrication process. NDS placed this function in a very secure built in self test (BIST) to be discussed later.

TNO also noted that there were several dead ends in the fabricated circuit board. These extensions make adding new components easier. However, they should have been removed due to lack of use. NDS was aware of their existence. There was reluctance on both the part of NDS and TI because removing the extensions only assists in preventing physical probing not electrical probing using a Focused Ion Beam (FIB) to be discussed later.

There were additional pads whose purpose was not identified by TNO. NDS *designed them for use when the chips are connected to the security server. These* are not exclusively used for test.

Wet etching: This process involves removing the upper, metal layers of the chip in order to expose the underlying structures. It is used to remove the layers selectively. This process is difficult but straightforward and can be performed on almost any integrated circuit. Removing a layer can make physical probing easier by reducing the thickness required to penetrate a component in a sublayer. Wet etching was difficult to perform because it frequently caused the chip to stop functioning. Inspection of a failed chip did not reveal the cause of the failure. After a number of unsuccessful attempts the scrambling blocks were identified.

6.2 Internal Probing Attacks

Probing attacks may be carried out by either inserting mechanical probes directly into the data bus or with the assistance of a Focused Ion Beam (FIB) system. A FIB system deposits tiny (5 μm x 5 μm) platinum probe pads on the bus wires. The FIB system works on almost any card however the expertise level is extremely high. It is possible to contract this service in a day's time for approximately $2,500 USD. TNO contracted with a Cambridge lab to perform this service.

Probing is the process of accessing the data as it travels across the bus. Probing is essential to reading the running code of an executing program and compromises the op-codes, jump addressed, and processed data. TNO reports that no deliberate physical protection methods have been found to prevent probing.

Probing can be made more difficult by implementing secure packaging and adding extra metal layers. Adding metal layers must be implemented carefully so that intrusion is noted and proper action taken.

Driving the chip using a PC and card reader carries out the analysis. TNO reports that no problems were encountered with tapping and collecting the bus information. The bus read was repeatable. Tapped bus information must be disassembled and analyzed to reveal the proper operation of the card.

Upon analyzing the disassembled code, TNO realized that the tapped data from the bus had been scrambled. Scrambling the data on the system bus is seen as a strong security feature. Further analysis revealed that data on the bus was unscrambled while the instructions were scrambled.

The chip employs scrambling in both hardware blocks and in op-code numbering. TNO never understood these techniques. TNO believes they had reverse engineered the scrambling blocks, however, their analysis was not completely accurate.

As TNO stated in their report, the FIB system discussed above requires technical expertise beyond the reach of most hackers. As stated above it is possible to contract this service out. TNO also attempted to implement direct probing that is similar to FIB pad probing but uses direct connections to the bus. This process requires no special hardware and may be in-house. This approach proved to be unsuccessful.

6.3 Hardware Components

The internal analysis covers both the physical hardware components and the security features of those components.

Busses: The busses employ non-orderly routing but this does not make reverse engineering much more difficult. The data and address bus connected to the memories can be easily located. NDS reports that this routing technique did slow down the hacks on P1. Further analysis revealed the presence of bus and address blocks. These blocks reduce the vulnerability of the simple bus structures.

Thompson uses a metal layer over the data bus wires. This can be made more secure by making the metal layer an active component, i.e. sending useful current thorough it. But this makes the chip more expensive. The present Thompson chip does not do this correctly. Thompson's ST19 will reportedly do it right. Siemens says it will follow suit. Philips says they will not make modifications to their chip.

ROM: The ROM consists of 16K Bytes and is made of physical transistors as seen under an optical microscope. The ROM should have been an implant, not physical transistors. TI took the definition of *implant* too liberally. NDS was not aware of the implementation until the TNO report was produced. TNO indicates that in reality, TI did NDS a favor with the transistor implementation because a traditional implant solution is easier to read visually by staining the surface.

The card executes out of both ROM and EEPROM. NDS assumes that all ROMs are readable. TNO states that reading the ROM is essential to reveal the original source code and to make a fully functional emulator. DIRECTV inquired as to whether other countermeasures could be taken such as doubling the size of the ROM and only using random locations. NDS indicated that this technique is possible but physical space was an issue and prevented such an approach. ROM design is also complicated by manufacturer reliance on a differential constant to account for an up to 40% error in the bus wire alignment.

Co-Processor: TNO could not find a function for a hardware block that they called a co-processor and questioned whether it was used.. This device is the integrated ASIC. NDS reports that it has a dense transistor based design and is extremely difficult to reverse engineer. TNO was confused by its constant power consumption designed by NDS. NDS indicated that this property was partially contributed to by luck. However, they said that cryptographic algorithms by nature have balanced designs. A detailed description of power analysis will be presented later in the report.

EEPROM: The EEPROM consists of 8K Bytes plus an additional row of 32 Bytes external to the two 4K main memory blocks. The extra row is covered with metal and TNO suspected that it was used to store security information. TNO never discovered the function of the extra row. NDS revealed that it was a security trick that replaced one of the internal rows through remapping the EEPROM memory. TNO identified 15 wires used to address the 8K plus 32 Bytes but did not verify which wire controlled the extra 32 Bytes. EEPROM is not encrypted.

RAM: The RAM consists of 384 Bytes with no embedded security features. Tricks were not employed due to schedule pressure. NDS did not realize that they would have an extra year to redesign the software after the hardware design was fixed. The introduction of scrambling blocks would have taken several months of so and would have pushed physical space constraints, but again NDS did not know they would have had an additional year. As a result the RAM was not encrypted or EEPORM.

The RAM blocks are made out of nonstandard TI components. Typically memory is made out of either 256 Bytes of 512 Bytes. Space constraints prevented use of 512 Bytes.

Scrambling Blocks: *Scrambling blocks are used to manipulate the data so that* it ~~is~~ *cannot be directly observed on a system bus.* While TNO initially did not expect anything to be scrambled, upon realizing that memory was scrambled, they began the long tedious task of reverse engineering the scrambling blocks.

TNO believes that they completely reverse engineered the scrambling blocks. However, they were not correct in their assessment. NDS stated that TNO was not successful in completely reverse engineering the descrambling blocks. TNO failed to discover the variability of the encryption keys. Different parts of the ROM are encoded with different keys. Cannot just send the encrypted code through the descrambled blocks to get the code as implied by TNO.

TNO was unable to discover the function of the T-Bus. This is used to modify the scrambling algorithm. Each time a different number is placed on the bus, the scrambling function changes.

NDS revealed that one of the most damaging items in the TNO report is the *presence and reverse engineering of the* scrambling and descrambling blocks.

Built In Self-Test: The test programs were built exclusively for NDS. TI may later use them for their other products (NDS stated that scrambling blocks will not be used in other products). NDS provided TNO with the assembly language test code. TNO was not able to enter test mode because they have not been able to decode the ROM image. Some manufacturers let you enter test mode using a secret key. NDS indicated that this in *not* the case for the TI chip.

EEPROM tests in the BIST were designed to be strong. The EEPROM is erased before running the EEPROM test. The contents cannot be externally accessed. External access attempts destroy the contents upon entry.

TNO found the ROM addresses to be sequentially addressed through use of a ROM CRC test function. This test will address each ROM location sequentially and calculate a CRC over the scrambled result. This test may be misused by an attacker to provide a complete listing of the ROM contents NDS reports that this was an interesting finding that could have been altered. This was not thought of when writing self-test code. Sequential addressing may help bypass ROM address descrambling. Reverse engineering of scrambling blocks is still necessary for access to intelligible data.

6.4 Optical ROM Code analysis

TNO indicated that optical analysis could reveal the complete internal program structure and when disassembled can lead to access to test routines and protocol attacks. The physical transistors were read and their value placed in a table that was mapped into the logical location in the memory map. A read process was automated to distinguish ones from zeros and to place the value in a table. The automated process required approximately 17 hours per run. Between 2 and 3 runs were necessary. The bit error rate was 10%, which is much too high to achieve meaningful results. Errors were induced in part due to variations in temperature over the long, 17 hour period. TNO demonstrated the concept however they never succeeded in completely downloading the ROM. They revisited this subject many times throughout the report and did not significantly improve the results. The hardware required to perform this task is approximately $150K USD and readily available.

There are not as many Pirates as you might think (approximately 13-15 groups worldwide). Only about 10%-15% possess the ability to read ROM. Hackers tend not to share information because they compete for business. All are not solely focused on DIRECTV. Hackers are able to spend much more time than TNO or any contracted external analysis organization. However, reading ROM is a difficult problem.

6.5 External Analysis

External analysis covers operating specifications of the chip, time manipulation, voltage manipulation protection, current analysis and differential power analysis. Each topic will be covered in turn.

Operating specifications: The upper and lower levels of the supply voltage are measured by executing the answer to reset (ATR) and the TI test script. The supply voltage is varied in steps of 0.1 volt. TNO reports that the operating range of the chip is between approximately 2.4 and 7.0 volts.

Frequency tests were performed by monitoring the ATR only. TNO reports that the frequency range is estimated to be between approximately 228 kHz and 10 MHz. The boundaries have been measured by changing the clock frequency.

Time manipulation: TNO reports that the chip is susceptible to manipulation of the power supply during read cycles of internal memories. A dip in the power supply during a read cycle from ROM results in incorrect data transfer from memory to the bus. The read operation returns all ones (FFh) instead of the expected stored value. The FFh read is caused by a tri-state condition on the bus. The behavior can be reliably repeated.

TNO writes that *timing* is an important aspect of this attack. The voltage dip and duration of the dip must be tightly coupled to the program flow. External events, such as I/O operations and careful counting of the clock cycles provide *handles* to time the voltage dip. Once a specific moment is known, the attack can be performed on similar cards with the same program without opening them. The preparation is,difficult, but the attack can be quite simple.

TNO writes that this timing attack was effective in reading ROM and EEPROM. RAM is not affected. The consequences are different for each type of memory.

- ROM: The bus value of FFh will be descrambled into a different value before it enters the processor, the value as processed by the processor depends on the address data and the T-Bus value and is therefore difficult to predict. This phenomenon may however still be misused by an attacker to divert program flow. When not carefully timed the program may run out of hand, abort or cause damage to the EEPROM data.
- EEPROM: Varying the voltage during an EEPROM read cycle may allow the attacker to manipulate data as processed by the processor. Other system attacks may be possible and are not addressed by TNO.

These attacks may be more of a concern if an attacker had access to a code listing and understood the scrambling and descrambling blocks. They could use the read reliability to get certain values. NDS sees this as a potential problem. This could further complicate analysis of attacks using jump instructions.

Scrambling was designed to obfuscate the fact that the ROM was readable. It was not designed to prevent a specific form of attack, e.g. to defeat differential power analysis.

Manipulation of the power supply during read cycles might also cause instructions to be skipped, which can create unforeseen instruction execution sequences and access to protected code. NDS has agreed to investigate areas where illegal jumps may result skipping instructions and revisit areas where illegal jump instructions may be executed, caused by descrambled FFh reads subject to illegal voltage levels. Dipping voltage may lead to disclosure of information or manipulation of access rights. These actions were not part of the TNO report as they are considered system attacks.

A single power glitch that causes a FFh read could be translated into a jump in to a location that has dangerous consequences. NDS did not analyze the code for this consequence. It is difficult to do because P3 has 16K of code. If you assume that 30% of the instructions are jumps, this leaves 1600 jump instructions and possible places to examine. It is an issue with the ROM code, which cannot be changed easily because it is constructed with physical transistors. Jumps to EEPROM can be solved more easily.

An attacker operating on anything but an HNS A box will probably kill the card when varying the voltage.

Voltage manipulation protection: NDS has out of specification circuitry to reset the card when voltage levels are out of a predefined range. Some variation is allowed for ease of operation with the number of IRD models in the field and varying subscriber environments.

Thompson Consumer Electronics (TCE) was given a waiver for their 2nd generation boxes that supplied Vcc a lower 3.5V than the required value 5V. This waiver requires all current and future DIRECTV smart cards to operate using lower than normal voltage.

Hughes Network Systems (HNS) A boxes required a special card that implements changes to the voltage levels as defined in the specification. The modification holds reset when Vcc falls and is implemented through a metal layer fix to the card. This modification may cause the card to be less reliable. It also allows an attacker to use this version of the card to further manipulate the voltage level. This card does not require the proper voltage sequence, which may make it easier for an attacker to vary voltage levels when trying to hack the card. Therefore, P3.2 is immune from Vcc out of range voltage levels. However, varying the voltage may cause the P3.2 card to reset, thereby, preventing extreme voltage manipulation (*PERRY WILL LOOK INTO IF THIS STATEMENT WARRENTS FURTHER REVIEW*). Knowledge gained from these attacks can be used to break other cards that are protected when voltage levels are outside defined thresholds. For more information on card versions see the section titled, *IRD Manufacturer and Mailout Cards* above.

Current analysis: The objective of current analysis is to identify the cryptographic function and keys by studying the supply current variations. TNO writes the internal execution of a program will cause a modulation of the supply of the current of a chip. The current profile is directly related to the internal program execution. Repeating sequences of shapes can be used to detect the execution of loops in the program. This attack is best used to defeat known algorithms.

TNO used both simple power analysis (SPA) and differential power analysis (DPA). The latter requires knowledge of the command structure and information regarding the underlying algorithm.

TNO performs current analysis on a macro level. In contrast, CR uses current analysis on a macro and micro level, which could be used to gain more useful information. Macro level analysis looks at 500 – 1000 instructions at a time while a micro level analysis looks a 1 – 2 instructions at a time. NDS is more concerned about micro analysis of the modified TI chip (The processor used in P3 is modified from the standard TI chip.).

TNO reported that there appears to be no countermeasures to power analysis. They analyzed power supplied to the core processor and ASIC (coprocessor). TNO was surprised that the ASIC used almost constant power. NDS reports that this is in part due to the nature of cryptographic algorithms and luck. TNO did not gain useful information using current analysis, because NDS uses non-standard, proprietary algorithms. They recommend more research in this area.

Even though there are no hardware countermeasures to power analysis, NDS believe that there are several software and protocol defenses. 1) the asymmetric signature algorithm is more difficult to attack. The card does not contain enough information to generate a message signature. 2) Checking message signature with pre-calculated value requires an internal hash of the message contents to be compared with a hash of the signature. The resulting pair of hashed values are compared. This makes it difficult for an attacker to determine where the differences occur in the pre-hashed input values to the hash functions. 3) When setting status bits, NDS maintains parallel code. That is, they put the result in another location when they appear to be performing an operation in what appears to be in one location, e.g. when ther appear to be setting bit 5 in byte 20, they actually set bit 5 in byte 21. This action is performed in select locations.

It would be good to put a requirement in the Px specification for the vendor to provide a power analysis countermeasure exclusive of the hardware platform capability.

6.6 Primary Attack Scenarios

TNO proposes two attack scenarios and gives an estimation of the skills and resources required to implement the attack. NDS agrees that these scenarios are likely.

Attack 1: Probing attack:
The steps required include:

1. General chip analysis
2. Reverse engineering of scrambler logic
3. FIB modification
4. Data tapping
5. Bus descrambling and disassembly
6. Conversion of running code Into memory-mapped code.

This form of attack requires general knowledge of micro electronics, moderate skill level required for probing on probe pads, and a high skill level in manual reverse engineering. TNO estimates that this form of attack requires approximately 3 months with 2-3 people.

The attack requires the following hardware: High-quality microscope, sub-micron probe station, logic analyzer, PC, and access to a FIB lab. Total cost $300,000 USD.

The attack results in obtaining program code and data that is executed by devices during the attack. This could be valuable information and used to make card clones. A complete clone requires ROM and EEPROM data.

Attack 2: Optical ROM analysis:
The steps required include:

1. Reverse engineering of decoded logic
2. ROM staining
3. Optical Imaging
4. Interpretation of images (including algorithm development)

This form of attack requires a moderate knowledge of micro electronics, Image recognition, microprocessor assembly code and intelligent image interpretation techniques. TNO did not estimate the time for this form of attack.

The attack requires the following hardware: High-quality microscope with computer controlled stepper table, PC and an image recognition system. Total cost $150,000 USD.

The attack results in obtaining the full program code and test code. This attack also provides Information on system functionality, which could be valuable information used to make card clones. A complete clone also requires EEPROM data that could be obtained through probing as described above.

NDS does not believe that any other firm or attacker could be more successful than TNO at ROM analysis.

6.7 Strong and Weak Aspects

TNO was not able to break the P3 card despite their claim that they have been able to break every other card they have attempted.

The following have been identified as *strong* aspects of the P3 design:

1. Internal bus scrambles
2. Difficult to mechanically probe (easy with use of FIB).
3. Little information found on chip surface
4. For a successful attack on the chip it is necessary to combine several fields of expertise.

The following have been identified as *weak* aspects of the P3 design:

1. ROM is made of physical transistors. NDS implemented scrambling to counteract this weakness.
2. Dead ends are present in the bus that makes direct probing easier; however, the chip structures are such that direct probing is very difficult.
3. Appears vulnerable to power supply variations during a read cycle. NDS will examine ramifications of possible jumps.
4. Data is in plain text. This is everything that goes through RAM and EEPROM. Could be intermediate values stored in RAM. This does not include values stored in registers. NDS because of time to market did not have time to add scrambling and descrambling for RAM and EEPROM. This would have been the first recommended change.
5. No secure chip packaging. NDS did not find a packaging method that they felt provided enhanced security while not introducing complications during manufacturing. In hindsight, they may have made another decision.

In retrospect, NDS could have done more to increase physical security of the chip but it was not known that they would have an additional year.

6.8 Defenses Not Uncovered

Special Function Generator (SFG): Another name for the ASIC. TNO completely misinterpreted the function of this component. TNO thought that this was a coprocessor that either this computed functions with constant power or perhaps this was not used. The P3 ASIC is completely different than P2. It is in the same family as GLA and could be in the same family as Sky P11.

If the algorithm is broken on an algorithm level then we have something to worry about. If its broken on a HW level then it may not be clear that that break would apply. FPGA used to emulate this ASIC would require a fairly sophistic circuit, i.e. a $100-$150 dollar version.

Adi designed the SFG. The design needs to be difficult to emulate in FPGA (Field Programmable Gate Array). Must be difficult to emulate in software and hard to reverse engineer. The ASIC contains scramblers and descramblers as well as special camouflage cells. It has many cells and is much harder to reverse engineer than the descrambling blocks. The component must be cryptographically invulnerable. The ASIC sits on the data bus. To use it as a peripheral one must reprogram the EEPROM.

Special Cells: There are no special cells in the scrambling blocks. Special cells exist only in the ASIC. It would have been better to put them in the scrambling blocks as well. NDS did the design work on the ASIC. TI did the design work on the scrambling blocks. NDS created circuits that seem to perform one function, but actually perform another, ex. an OR gate may look like an AND gate. Special cells are the same size as normal cells and are usually placed in a *cryptographically difficult spot, i.e., in a place that affects many bits.* If it were put in a place where only one bit changed, the special cell would be easy to locate.

Opcode Tricks: Two classes. 1) Simple instruction,swap, e.g., exchange subtract with add. 2) Make a new instruction. Both techniques can be used simultaneously. Can take made up instructions and place with real instructions. Or, can transform opcodes. Also, can randomize addresses.

EEPROM tricks: TNO did not understand the extra 32 bytes. NDS replaced a row in normal memory with the extra 32 bytes. There are bits in EEPROM that are stuck at 1. An over the air message may tell the card to put a 0 in a certain location but the card would write a 1 in a position where the bit should be stuck. A hacked card would put a 0 there. NDS checks if a 0 exists in this location, if so, they can take any one of a number of actions, including issuing a kill card.

Others:
Five level encryption: hardware - scrambling blocks; and E1-4 – so attacker cannot place data in the card.

E1: Checksum on certain areas of data. Common algorithm for all cards.

E2: Encrypt whole packet. General or group encrypted CAP. Byte for byte running encryption using ASIC.

E3: No data coming from outside is stored as received over air. Data is encrypted uniquely per card and different for each reset of card, even if the same data is sent. Each time the card is reset, a new key is generated using a random number as the key. Since a new key is chosen each time the card is reset, the contents changes as a function of the new key. A hacker analyzing the memory contents would see different data coming out of RAM making it difficult to make sense of the data. The encrypted contents are used for each RAM read/write operations. This operation is performed in software.

E4: Similar to E3, but for EEPROM. Fixed key per card.

General tricks in industry include implementing bus bit-order swapping.

7 Security and Cryptography Research Relationship

NDS has two cryptographic experts in Adi Shamir and Aviad Kipnis. Adi indicates that Aviad is the best student he ever had. Aviad has a military background and like Adi is an NDS employee. The two are used almost exclusively for cryptographic algorithm design including the ASIC function.

Shamir reviews the cryptographic algorithms and the DDT philosophy. He does not participate in the internal code review.

Historically, most attacks on DIRECTV have been protocol attacks not cryptographic attacks. Protocol attacks are possible through coding errors (bugs), unexpected execution sequences, and other unattended actions.

GLA initiated a relationship with Cryptography Research (CR) in which they requested a black box relationship using their P1 card. They have subsequently requested that CR participate in other technical discussions and reviews. DIRECTV has subsequently initiated a relationship with CR. DIRECTV has requested that CR conduct a black box evaluation of the P3 card. Little technical information was given to CR in preparation of the P3 card. The review is scheduled to be complete by early May.

CRs strengths are in Differential Power Analysis (DPA). NDS believes that CR is good at it but only with known algorithms. NDS also indicated that NDS, IBM and Cambridge are also extremely competent with DPA. Yossi has a related paper that he would email. NDS does not feel that CR will be able to learn much from their external attacks. However, NDS indicated that they believe that CR has more capability using internal attacks than they may let on. This option results from their discussion in the New York meeting facilitated by GLA in Jan 1999. NDS acknowledged that an inappropriate attempt to contact CR was made without GLA participation. DIRECTV discussed the new openness in the relationship between DIRECTV and GLA and that technical information beneficial to both companies may be shared.

NDS has high regard for Paul Kocher. They feel he is good at external analysis. Paul's downside is his strong opinions regarding open design process, which NDS (via Adi) strongly believes is inappropriate in the broadcast threat environment.

Paul does not think that a code review for GLA P2 would be as beneficial as a review of the threats that the system was designed against. CR would not perform the review, rather they recommend another company (Infogard).

NDS will support a third party code review for DIRECTV as long as:

1) it does not postpone the contract,
2) it does not delay change out of P2,
3) NDS receives assurance that IP will be protected by third party, and
4) Not a competitor to NDS. A competitor produces CA systems. *(can't read notes on this one. had something to do with third party not selling bugs to hackers)*

RANDOM THOUGHTS and NOTES:

DPA can be partially defeated by randomizing the bit positions of the key.

Intel writes regular code and sends it to a tamper resistant code generator.

8 Summary

To be completed by NDS