Countermeasures for Attacks on Satellite TV Cards using Open Receivers

Lishoy Francis, William G. Sirett, Keith Mayes, Konstantinos Markantonakis

The Information Security Group - Smart Card Centre,
Royal Holloway, University of London,
Egham, England, TW20 0EX

{l.francis, w.g.sirett, k.markantonakis, keith.mayes}@rhul.ac.uk

Abstract

Digital content providers seek to restrict usage by implementing conditional access. One such scenario is the security aspects of digital video broadcast (DVB-S). There has been a history of attacks on this technology to circumvent any security measures and some techniques have been countered by the deployment of customised/provider specific receivers. However, this leads to less choice and the duplication of equipment at the customer level. Open satellite receivers have been introduced to allow a single user to access several different services from a single piece of receiver equipment. These boxes provide a highly configurable environment with software emulations of conditional access systems that is open to abuse. The internet has allowed communities with in-depth expertise to grow up around open receiver equipment; effectively communicating attack methods as they evolve. A new level of emerging attack is a card sharing by which one legitimate user colludes to provide protected content to a larger group of illegitimate users. In this paper we propose countermeasures to protect DVB-S content against this species of attack by enforcing behavioural contracts and correct usage guidelines within the smart card.

Keywords: DVB, satellite content, attacks and countermeasures

1 Introduction

Television was and is traditionally broadcast using an analogue architecture. However, this is restrictive in terms of scalability, quality of signal and bandwidth. Digital transmission means that more channels can be broadcast with no compromise to quality. For example, the UK government is planning a digital change over within the next five to ten years (Digital Television Project Team, 2004). There are several differing methods for the delivery of digital television and this paper focuses upon Satellite or Direct to Home (DTH) architecture. As outlined by Francis L (2004), DTH involves an earth station to uplink to a satellite, transponders on the satellite receive the signal, translate the frequency and amplify before down-linking the concentrated signal to earth receivers within the footprint area. The down-link is received using a Low Noise Block (LNB) mounted on household dishes and decoded with an Integrated Receiver Decoder (IRD) more commonly known as a Set Top Box (STB).

Digital broadcast via satellite represents £3.5 billion market revenue in the UK with an Average Revenue Per Use (ARPU) at £50 annually according to estimates from the DVB project (DVB worldwide, 2004). With this money security concerns come and not without justification. The threat from piracy can cast a shadow on tens of billions of pounds taking into account worldwide providers (NDS 2004). In order to protect their investment and revenue streams, controlling companies must encrypt the digital content. Many providers follow the DVB-S standard and tailor the specific encryption to their own particular needs (ERT 289 1994, ERT 154 1994).

This architecture has been attacked in the past using illegitimate receivers and, post smart card issuance, cloned cards. Each provider's receiver differs and this tailoring, in effect, limits consumer choice as a separate device is needed for each service. The market has responded by providing open satellite receivers. The justification is that a user can purchase several provider packages and access the digital content via one Set Top Box. Open receivers have developed to such a degree that they offer a highly configurable environment, rather a powerful Linux workstation with satellite communication functionality than a dedicated consumer device. They can offer fundamental access to the smart card and Conditional Access Module (CAM) which can be used maliciously.

The black hat community is effectively attacking the satellite security measures by abusing open satellite receivers. The aim of this paper is to review the current state of affairs and, through practical experimentation with different attacks, propose countermeasures for the future. Firstly, a review of open satellite receiver technology is documented. Followed by a discussion of the existing attacks in the wild, the process of compromising an open satellite receiver, details of an emerging Card Sharing attack and the proposed countermeasures that could be taken both in the overall architecture of DTH and on smart cards.

The authors omit vital details on attacks and the reconfiguration of open receivers as the focus of this paper is to put forward countermeasures for identified types of attacks.

2 Open Receivers

An open satellite receiver is a very sophisticated re-configurable satellite receiver that offers the ability to use several satellite provider services at the same time. To facilitate this, receivers come with more than one CAM and smart card slots. What is justified to provide viewers with more choice is now offering a great deal of flexibility to circumvent security. These pieces of equipment are open to abuse and a thriving community is using them to view encoded DVB signals which are otherwise subscribed for (Rysdale L, Paul B and Hulyalkar S, 1996). Detailed next is the specifics of open receiver functionality, the costs and availability.

The receiver hardware is more than a consumer electronic device of the order of the provider receivers, DVD players etc. It is more akin to a computer with built in MPEG 1/2 decoder and a variety of smart card readers. The receiver comes preinstalled with software commonly know as an image which is comprised of an operating system, usually Linux, a graphical user interface and plug-ins. The image resides on the EEPROM or flash memory of the receiver. For the purposes of experimentation, a third generation receiver called DreamBox 7000 S120 (DreamBox Multimedia 2004), was used. It is this device's functionality and capabilities that are detailed in the following paragraphs.

Such a receiver supports the following functionality:

- Alternate Firmware or images
- Emulation of Smart Card and CAMs
- Secondary storage device and other USB storage tokens
- Plug-ins
- Networking
- DVB/MPEG1/2 support
- Keyboard and complex input devices

Plug-ins refers to software which functions independently from other software modules. For example, an image can be run from a USB device or hard-disk. The storage capability of these receivers is not to be under-estimated; the model acquired came with pre-installed 120GB hard-disk and could very easily be expanded. This, coupled with the Linux operating system, allows for content to be streamed to the disk and distributed in many different un-encrypted formats. This is the cause for concern, especially when considered alongside the extensive networking capabilities of many receivers. The DreamBox has a network card for Ethernet communication, a serial port and built-in modem to mimic standard receiver functionality of communicating a return path to the provider for additional services. Servers can be run and have the general functionality of a computer.

There are a wide range of open receivers freely available on the market and our highly configurable DreamBox was attained for as little as £400. The range of equipment available is extensive and all provided under the legitimate guise of trying to aid multi provider functionality.

3 Satellite TV Attacks

In this section we are going to document existing satellite TV attacks, the black hat community surrounding the technology and the existing attacks that exist in wild along with an emerging card sharing attack.

3.1 Introduction

There is a variety of methods for circumventing broadcast security varying in degrees of sophistication. The method selected by the attacker relies on several key factors; what service is being selected and its level of security and the expertise of the user. Some simple attacks are pre-built into the equipment but other requires a serious level of understanding to be undertaken. The dissemination of black hat knowledge will be discussed after the classes of attack have been identified and particular methods detailed in brief. Once again it is important to note that the brevity of given information is enforced to avoid educating an already pervasive community.

3.2 Black Hat Community

The community surrounding this technology is widespread and growing fast. Even tentative steps into the Internet using website and forums unveil in-depth expertise and an effective information dissemination framework. There are forums for different purposes; beginner boards where questions can be answered, advanced boards for the programming of new attacks, advice sections to discuss new equipment (receivers, dishes, CAMs and cards) and open discussions on related news and events. Worthy of note is the secretive nature of some of the more established communities indicated by the ever moving virtual location of some of the internet resources and a structure modulated system. After a member has given enough advice or shown to be skilled, above that of the average attacker, they are elevated into more selective groups to discuss advances made. Due to the very nature of the Internet; it would be very difficult to eradicate these communities as is the case with other more illicit types of Internet communities.

3.3 Card-less Attacks

The most basic form of attack is a standalone card-less attack. To understand how it operates it is first necessary to define the components of a Condition Access System (CAS) (EBU Project Group B/CA, 1995). A CAS compromises of a Conditional Access Module (CAM) and a card. Some CASs only has smart card elements and other only CAM but it is assumed that the CAS has both elements in respect to the discussion of abstract security.

Users must have both elements plugged into the open receiver to decode the encrypted DVB signal.

However, emulation exists and can provide the functionality of CAMs and smart cards in software. Once the image is flashed and the plug-in is added to the open receiver, the emulation needs to be enabled and the weaker CAS systems can then be viewed. Practical experimentation showed that a number of widely used CASs were easily broken (Francis L, 2004).

It was shown that more advanced CASs proved resilient to this attack and required more complex method of attack. For example, the Card Sharing attack described later on in this paper. However, a strong factor is the ease of which an attack can or cannot take place. This additional security could be enough to deter a casual attacker from assaulting the stronger CASs and focus on the open receiver's built in capability to attack the weaker ones.

3.4 Card Sharing

The card sharing attack is highly sophisticated in comparison to the card-less attack. In this method the security of the CAS is bypassed lucratively. Here a subscribed user, employing compromised open receiver software, seeks to collude and provide access to a larger group. It is believed that this attack will become central to the use of open receivers in the future and the ease and spread of the shared card attack will continue to evolve. The card sharing attack will affect the industry in the long run by siphoning at a steady rate the industry revenue and potential customers. It is fair to assume that an individual willing to spend the sum of money required to bypass the security would resign to subscription if faced with unbreakable security.

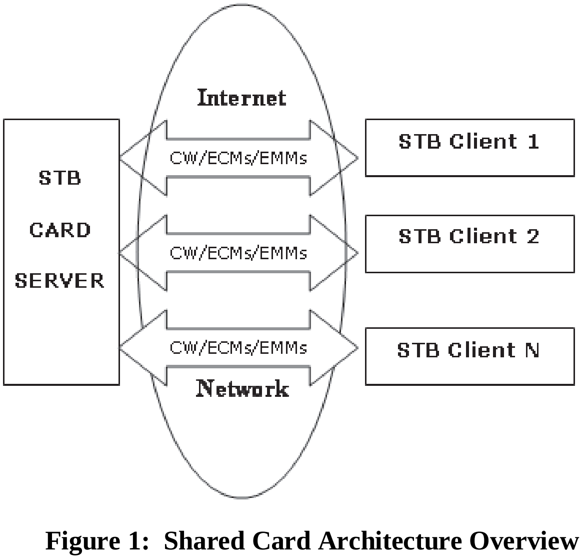

Figure 1: Shared Card Architecture Overview
(Francis L, 2004)

3.5 Feasibility

To develop attacks on DVB is a fairly complicated undertaking and requires a depth of knowledge that is not widely held. However, black hat communities spread tools that remove the attacker from the detail of the underlying technology and this is a key factor to the increasing widespread use of open receivers in an illegal manner.

Furthermore, an attacker can experiment in the relatively certain knowledge that they will not be caught. The open receiver does not communicate back to the provider unless there is a specific attack involving communication and the anonymity of the Internet coupled with readily available secure content (from a dish) enforces this.

To conclude, it is technically accessible to new users with limited understanding being given the help and tools from more knowledgeable attackers. In addition to these facts, there is the attractive benefit that their activities can go relatively undetected and enter the scene for a relatively low cost. The feasibility of undertaking an attack is considered high.

4 Reconfiguration of Open Receiver

As a demonstration of the simplicity of performing some card-less attacks, the open receiver can be reconfigured to break lightly encrypted services with little more than the tools provided by the black hat community. The specifics of the software is omitted to prevent this section from becoming another how-to introduction in to “hacking”. The equipment involved:

- A DreamBox S120
- Desktop PC
- Dish
- TV Tuner Card

The DreamBox was assigned an IP address and connected to the computer to upload the existing image. Once complete, the original image on the receiver was deleted and a compromised image was loaded. The open receiver's basic configuration is changed and configured further with respect to the basic satellite details. The satellite configuration list is loaded and connected to a pre-decided satellite. After enabling certain built-in functionality, the encoded DVB programmes were available without any subscription .

Only the simple systems were broken and no card was needed. Tougher systems need card and CAM to be present to decode the signal. With some relatively small monetary outlay and some time to spend, these pieces of equipment can be purchased. However, there has emerged from the wild a card sharing attack which will make the possession of specific CAMS and cards irrelevant.

5 Card Sharing Attack

The card sharing attack is a more sophisticated class of attack compared to the stand alone card-less attack. A card sharing attack was outlined by Kuhn M (1997) however his attack does not involve re-configured open satellite receivers. The essence of the attack is to allow one user with a legitimate card to collude with an unrestricted number of illegitimate users to provide unauthorised access to protected content to all.

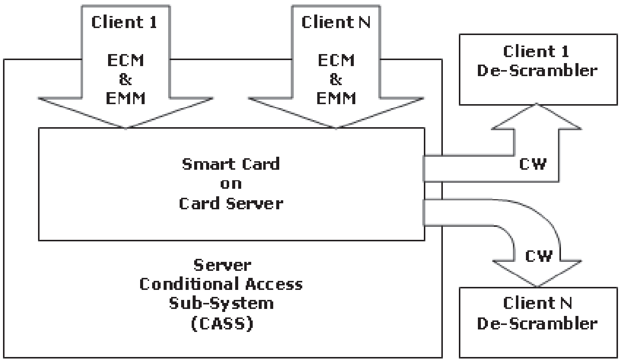

Figure 2: Card Sharing Attack (Francis L, 2004)

The user with the subscribed card runs a Card Server on their reconfigured open receiver and listens for client communication on a given port. Entitlement Management Messages (EMMs) and Entitlement Control Messages (ECMs) are sent by the clients to the server which in turn decrypts and returns the control words used to scramble the content. The server carries out a unilateral authentication of the clients using the legitimate card and continues to exchange ECMs and EMMs allowing clients to access encoded DVB programmes without subscriptions. The Card Server gives each client a thread and this is the only limiting factor of the network. The Server can only support as many clients as the card allows. Since cards have restricted computational, storage and communicational resources, it can be assumed that there are a finite number of possible users authenticating on any given card.

The knowledge to perform this attack is available through the black hat community and the reconfiguration of the open receivers is fairly simple for the clients and slightly more complex for the server. The extent of the attack really depends upon the implementation of the Conditional Access System (CAS). The compromise of ECM in turn results in the compromise of a control word. The compromise of an EMM results in the compromise of the new master key. If the new master key is derived from the original master key then the hack is sustained over a short period of time. However, if the new master key is not derived from the original key, the attack will sustain until the next card change.

6 Countermeasures

The purpose of this section is to outline countermeasures to prevent the successful attack of DVB broadcast. A main driver behind the attacks comes from the effective manner in which information is shared about the subject. If it were possible to stem this communication then the spread of attacks would slow. However, it is believed that it is unfeasible to attempt to restrict a group’s communications, especially considering the underlying nature of the Internet.

A key factor is that the proprietary receiver (Lievart N, 2001) or open receiver comes into the possession of the user; and therefore cannot be considered trusted. The user domain is an untrusted one and could be subject to standalone or colluded user attacks. The introduction of smart cards into the framework aims to provide trust in an unsecured environment. It is believed that the answer lies in the smart card, this is the only trusted entity at the client end and these could be enhanced to prevent existing and card sharing attacks. The countermeasures currently undertaken, the deployment of STB with smart card and CAMs to enforce condition access, need enhancing with card countermeasures to address some of the problems.

6.1 Card Countermeasures

As a countermeasure to address the card sharing problem it is proposed to enforce correct behaviour within the card. The essence is that the card has knowledge of behavioural contracts and once violated it would deny services to the accessing box.

6.2 Behavioural Contracts

This situation or environment is not overly complex in terms of communication to and from the card. The card needs to have an idea of what process of instructions it expects to receive over a given period of time. By analysing behavioural contracts built into the card or learnt over time, the card can ascertain anomalous behaviour and possibly prevent/stop attack. The smart card requires a state-memory and be able to process state transitions to support this functionality (Mayes K, Markantonakis K and Sirett W, 2004).

6.2.1 States and Transitions

For example; given that the card expects one process of a particular type every five minutes and that process always includes four exchanged Application Protocol Data Units (APDUs) in a predetermined order. The card state transition is induced by the receipt of certain messages and can only flow in one direction until the card returns to a stateless state.

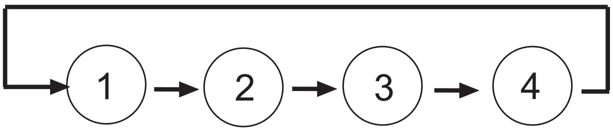

Figure 3: Example State Diagram

The card would not accept anything other than the messages in that order and any deviation would result in a reset, a challenge-response exchange or perhaps the disabling of the card itself. During the authentication process, a check should be made to see whether an anomalous event has occurred or a flag has been set. If this test result is positive, then the card has to go to reset mode and stop processing. Otherwise the attacking user could reset the card and continue usage. This countermeasure applies the knowledge of behavioural contracts to the authentication process of the smart card. There is the possibility of perpetrating a denial of services attack on behaviourally restricted smart cards but the essence of this countermeasure is to deny services. It is therefore not surprising that this functionality can be portrayed as a weakness. Further experimentation will need to be performed to enforce legitimate denial of services and the consequences for illegitimate attacks.

6.2.2 Run Time Statistics

Mayes K, Markantonakis K and Sirett W (2004) suggest that a contract may be broken with improbable rather than impossible behaviour. A further consideration is that of the number of given processes for a period of time. For example, normal usage of an authentication process may be one authentication every two minutes. A card sharing attack might involve any number of card-less boxes communicating with one central card, accessing the card very regularly to authenticate messages, and this behaviour could be noted and prevented. However, the smart card micro-controllers depend on the applied clock signal (Rankl W, 2004) and hence, the smart card has no internal source to keep track of time independently from the open receiver.

Timing Concept: The card could demand to know a time stamp from the box and ensure that this timestamp is in the future compared to the last timestamp. The timestamp would need to be authenticated in its own right, perhaps by a digital signature (Paterson K, 2004) using private key or similar cryptographic function. The time interval for data access can be calculated in terms of applied clock signals; the software modules implemented on the card could be aware of the frequency of data access. Perhaps a dynamic counter could be implemented or a hash of the last piece of received data. The specifics are currently being explored in a series of experimentations.

The idea is to understand the card access rates and establish the baseline behaviour. An interesting area for exploration is the possibility for the card to determine normal usage after issuance as described by Mayes, Markantonakis and Sirett (2004). Different cards in different situations would experience different behaviours. An ideal solution would be a smart card that could establish over time behavioural contracts and enforce them when usage exceeds certain values obtained post issuance. This remains an open problem and one for further investigation.

6.2.3 Application to DVB-S

Now it has been suggested that behavioural contracts can countermeasure both improbable behaviour and impossible behaviour; it is important to suggest how this can be applied to the infrastructure described. Discussed in this section is the method by which contractual enforcement can be applied to smart cards used in open receivers. First it is important to outline the communication involved in DVB Conditional Access (CA) in more detail using Francis L (2004). The DVB conditional access message format specifies a header structure for the CA messages. These messages include Entitlement Management Messages (EMMs) and Entitlement Control Messages (ECMs) in conformance to the MPEG section data. ECM and EMM are transmitted Over-The-Air (OTA) long with the video and audio signals. The idea is to carry a control word (CW) inside an ECM encrypted with a secret key. This secret key is held inside the smart card. The CW which is used to decode the signals is obtained by decrypting ECM using the secret key. The ECMs carry operational information and the EMM usually carries the management information such as a new secret key.

In a card-sharing attack, all the ECM and EMMs are sent from the group of colluded users to one card. It is straight forward to understand that if one hundred users are involved, the card at the centre of the conditional access card server will have to process one hundred times as many messages as normal. So it is proposed that the card is issued with a preset number of ECMs, messages containing the new encrypted control words, to be processed an hour. If this is exceeded then predetermined actions will be performed to deny service. An interesting proposal is that the card can perform dynamic configuration. From issuance the card can determine what a benchmark for usage is and any drastic deviation from this will result in anomalous behaviour being flagged.

However, further investigation is required into the specifics of this dynamic process as it is open to attack. A brand new card could be maintained at an unusually high number of processes from issuance and therefore be used in high-capacity attack such as card sharing.

7 Conclusions

In this section we propose to draw the conclusions the work previous presented. This includes conclusions about the future of the open receiver market, the black hat community and proposal to counter attacks and the effectiveness of behavioural contract functionality in combating card sharing. Finally, future work will be outlined to complete this paper.

Open receiver technology will continue to improve; this is due to the thriving community's demand for improved equipment as the sophistication of attacker's skill set improves. The black hat community surrounding open receivers will also grow. This relies on many factors but in short the Internet provides them with the anonymity and information dissemination required to educate new members, spread new techniques and discuss the challenges at hand.

The feasibility of attacks will remain high and increase over time. The standalone attack will continue to spread, if the CASs does not change the ease at which they can be performed and, as a result of an effective community, developing tools make it attractive to new comers. The costs of equipment will continue to diminish making the situation worse. Card sharing attacks thought complex at the moment will improve as the community refines their tools. In the foreseeable future, this type of attack will spread and seriously effect business. Once again the education provided by communities, cheap equipment and reward if success drives this activity further.

The concern comes in the form of card sharing as the biggest threat to future broadcast security. It can be assumed that smart cards are the only trusted element at the client site, and coupled with tamper resistant attributes, cryptographic functionality and proposed dynamic behavioural contract enforcement, they the key to future protection. There remains extensive academic scrutiny of the underlying principles of card sharing and behavioural contracts. Further practical experimentation will need to be undertaken to extensively prove the effectiveness of the proposed countermeasure in reality. It can be highlighted that the additional processing of behavioural contracts and the storage of states and transitions will have an additional cost after implementation. However, this cannot be identified without further investigation. The event set being monitored in this situation is greatly reduced when compared to the event set of a fully functional multi-application smart card (i.e. a SIM card) and the cost may be proved to be mostly negligible.

To conclude, it is strongly believed that the smart card infrastructure currently deployed will be successful in the future if the security issues mentioned before are explored and the proposed countermeasures are implemented.

8 References

Digital Television Project Team: Department of Culture, Media and Sport. http://www.digitaltelevision.gov.uk. Accessed Aug 2004

DreamBox Multimedia Worldwide: http://www.dream-multimedia-tv.de/Bereiche/Produkte/DM7000.php. Accessed Aug 2004

DVB Worldwide: DVB Project. http://www.dvb.org/index.php. Accessed Aug 2004

EBU Project Group B/CA(1995): Functional Model of Conditional Access System, *EBU Technical Review.*

ETR 154: Digital Video Broadcasting (DVB): *Implementation guidelines for the use of MPEG-2 systems; Video and audio in satellite, cable and terrestrial broadcasting applications.*

ETR 289: Digital Video Broadcasting (DVB): *Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems.*

Card Technology Today (September 2003): The Pay TV Market, *Survey*.

Francis L (2004): Security of Satellite Smart Card Encryption Systems & New Risks Introduced from Open Satellite Receivers. *MSc Dissertation. Information Security Group, Royal Holloway, University of London*, London. UK.

Kuhn M (1997): Attack on Pay-TV Access Control Systems. *Security Seminar talk. University of Cambridge*, London, UK.

Lievart N (2001): IA STB Security Issues. *IRDETO*

Mayes K, Markantonakis K and Sirett W (2004): SIM Enforcement of Mobile Terminal Behavioral Contracts. *Internal Seminar paper. Smart Card Centre, Royal Holloway, University of London.* London, UK.

NDS (2004): Smart Cards in Satellite TV. *OPT11, MSc Information Security Lecture, Information Security Group, Royal Holloway University of London.* London, UK

Paterson K(2004): Introduction to Secure Protocols. *IC3 Lecture Notes, MSc Information Security, Royal Holloway University of London.* London, UK

Piper F, Murphy S (2002): A Very Short Introduction to Cryptography. OUP

Rankl W and Effing W (2004): *Smart Card Handbook.* London, John Wiley & Sons.

Rysdale L, Paul B and Hulyalkar S (1996): Digital Video Broadcasting: Satellite Specification. *Philips Journal of Research Vol 50 No. 1-2.*