A Comparison between satellite DVB conditional access and secure IP multicast

H. Cruickshank[1], M.P. Howarth[1], S.Iyengar[1], Z. Sun[1]

***Abstract*— Security of satellite data is becoming an important issue. The DVB (TV broadcasting) Conditional Access system used in satellite broadcasting has however been surrounded by controversy for many years due to the spread of counterfeit smart cards, and this paper examines the weaknesses of current DVB-S security. We provide an alternative solution to secure multicast services over satellites using IPSEC and a group key management system called GSAKMP.**

***Index Terms*— Security, Conditional Access, multicast, DVB-S, DVB-RCS.**

I. Introduction

There probably exists no other application of satellite technology that is as well known as satellite broadcasting [1], [2]. The Digital Video Broadcasting (DVB) system has been designed with a modular structure, based on independent sub-systems, so that a variety of DVB systems (such as DVB-S: satellite, DVB-T: terrestrial, DVB-C: cable) could maintain a high level of interoperability. The challenge for the next generation of satellite access systems is to define a common basis for efficient integration of satellites in IP-centric telecommunication networks. One important area of integration is the communication security system. Security can be provided at various such satellite link level (such as DVB-S conditional access); or security can be provided at the network level such as IPSEC. Both link and network level security have their strong and weak points, they can work together to provide a stronger security system.

However, DVB Conditional Access (DVB CA) has been surrounded by controversy for many years due to the spread of counterfeit smart cards. For example, in late 1999, Italy was flooded with cheap counterfeit cards that enabled viewers use Canal Plus for free [3]. In March 2002 Canal Plus Group filed a US federal lawsuit against rival NDS Group, accusing it of cracking its digital television smart cards and putting the confidential information on the Internet, "permitting theft of digital television on a massive scale" in Europe [4]. Therefore there is a need for a radical change in the DVB CA system.

The work in paper is conducted within a European project (within the Information society Technologies, IST, programme) called SATLIFE [5] that examine the new services and applications over an On Board Processing (OBP) satellite system called Amazonas. It is based on the AMERHIS OBP payload developed by the European Space Agency (ESA) and operated by Hispasat [6]. Amazonas system integrates and combines both DVB-S (broadcast) and DVB-RCS (satellite return links) into one regenerative multi-spot satellite system.

In this paper, we examine the current DVB-S one-way conditional access system and review its weaknesses; we then focus on network level security and providing group security using IPSEC and the related group management architecture in the IETF group called MSEC (Multicast Security) [7]. We present a scalable secure IP mulicast system that can used to secure satellite broadcast and interactive services.

II. The current DVB-S broadcasting (one-way) access control system

Conditional Access (CA) is a service that allows broadcasters to restrict certain programming products to certain viewers, by encrypting the broadcaster's programmes. Consequently, the programmes must be decrypted at the receiving end before they can be decoded for viewing. CA offers capabilities such as pay-per-view (PPV), interactive features such as video-on-demand (VOD) and games, the ability to restrict access to certain material (sports or film channels, for example) and the ability to direct messages to specific set-top boxes (perhaps based on geographic region).

Conditional Access used in the DVB system [8], [9], [10] includes three main functions: scrambling / descrambling, entitlement checking and entitlement management:

- The scrambling/descrambling function aims to make the service incomprehensible to unauthorised users. Descrambling can be achieved by any receiver having an appropriate descrambler and holding a secret Control Word (CW). Scrambling can be applied to service components, either using a common Control Word or using separate Control Words for each component.
- The entitlement checking function consists of broadcasting the conditions required to access a service, together with encrypted secret codes (the Control Word(s)) to enable the descrambling for authorised receivers. These codes are sent inside dedicated messages (DVB tables) called

[1] Centre for Communication Systems Research, University of Surrey, Guildford, UK

Entitlement Control Messages (ECMs) and these are carried in the ensemble.

- The entitlement management function consists of distributing entitlements to receivers. There are several kinds of entitlements that match different means of subscribing to a service: subscription per theme, level or class, pre-booked pay-per-programme or impulse pay-per-programme, per service or per time. This information is sent inside dedicated messages called Entitlement Management Messages (EMMs) and these may be carried in the same ensemble as the scrambled services or by some other means.

The control and management functions (ECM and EMM) require the use of stronger security measures than the CW. Therefore secret keys and cryptographic algorithms such as Digital Encryption Standard (DES) are used to encrypt the control and management messages, while simpler scrambling algorithms are used to encode actual media streams using the CW.

A. *Data scrambling in DVB-S*

The CA service can scramble the programming data either at the Packetized Elementary Stream (PES) level or the MPEG-2 Transport Stream (TS) level. Currently, the preferred option is scrambling at the TS level. When a CA service is included, the architecture is modified as shown in Fig. 1. The CA system resides between the multiplexer and the modulator. The multiplexer (Mux) now combines the EMMs and ECMs along with the video, audio and data into a single DVB transport stream. The modulator takes the scrambled signal and modulates it for transmission to the satellite. The CA system is composed of several specific modules:

- The Smart Card Processing System: contains information about the secret information stored into consumer smart cards or set-top boxes, including in particular each Smart Card's secret key. This module is sometimes integrated in the SAS.
- The Subscriber Authorization System (SAS): processes the different viewing authorisations given to the subscribers and uses them to generate adequate EMMs and ECMs. The SAS also generates the service key, transmitted in the EMMs.
- The Control Word Generator: creates the Control Words.
- Two encryption engines (often implemented by the same software): used to encrypt the service key transmitted in the EMMs, and the Control Words transmitted in the ECMs.
- The scrambler: scrambles the payload of the packets composing the transport stream, using the Control Word. The scrambler usually scrambles the packets containing the picture and audio information and sometimes some packets containing data. Packets containing EMMs and ECMs are not scrambled. The preferred implementation of the scrambler is in the multiplexer device. Stand-alone scramblers also exist.

In addition, the Conditional Access system interacts with the Subscriber Management System (SMS) that holds all the data related to subscribers, running subscriptions and payments. SMS in turn interacts with the Billing and Customer Care system to generate revenues. The SMS tells which programmes subscribers are authorised (entitled) to view.

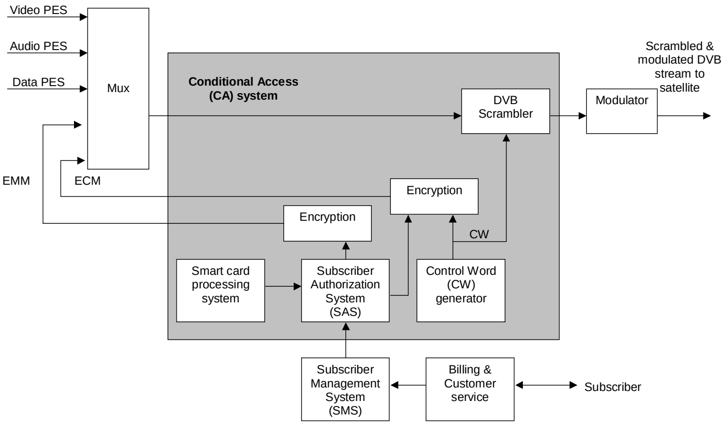
Video PES
Audio PES
Data PES
Mux
EMM
ECM
Conditional Access (CA) system
DVB Scrambler
Modulator
Scrambled & modulated DVB stream to satellite
Encryption
Encryption
CW
Smart card processing system
Subscriber Authorization System (SAS)
Control Word (CW) generator
Subscriber Management System (SMS)
Billing & Customer service
Subscriber

Fig. 1 General architecture for Conditional Access system (scrambling)

B. *Data descrambling in DVB-S*

At the receiving end, the set-top box descrambles the programme streams and decodes the MPEG-2 data for viewing as shown in Fig. 2. The tuner portion of the set-top box receives the incoming signal, demodulates it and sends the resulting data to the transport stream generator. This reconstitutes the transport stream, which is passed to the MPEG-2 decoder.

Fig. 2 also shows the DVB descrambling system. However, it should be noted that the DVB standards do not specify the smart-card electronics or algorithms, and therefore the system described here is simply a typical example. The encrypted session key, or Control Word, carried by the ECM, is related to particular programme material. This key allows the transport stream to be descrambled so that the viewer can see a particular programme or view the programme material for a particular session. As Fig. 2 shows, the service key (transmitted in the EMM) is sent to the smart card, where it is decrypted using the Smart Card key. The decrypted service key is then used as the key to decrypt the session key or Control Word (transmitted in the ECM). It is this CW that is the key for the DVB transport-stream descrambler.

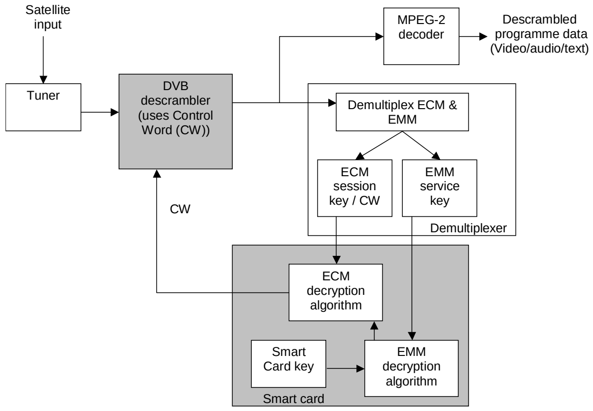

Fig. 2 DVB descrambling in a typical set-top box

C. *Weaknesses of DVB Conditional Access*

The DVB specification specifies the algorithm to use to scramble a DVB stream: it is called the DVB Common Scrambling Algorithm (DVB-CSA). This algorithm is standardised but is not public [11]. Technical details of the scrambling algorithm are only made available to bona-fide users upon signature of a Non-Disclosure Agreement (NDA) administered by the Custodian (ETSI). Having a non-public security algorithm does not inspire confidence because any weaknesses in the system cannot be scrutinised publicly. This compares with the current activities in IPSEC and the Internet community, which are all focused on open algorithms that have been in the public domain for many years. It is our view that the same principle should apply to future versions of DVB-CSA and other future DVB security systems.

In addition to the open system issues, let us analyse the weaknesses of the existing DVB CA system. The following is a summary of the CA system procedures:

1. An EMM containing a new service key is encrypted with the Smart Card (SC) secret key. Each SC key is unique, and so EMMs are effectively unicast (not broadcast) to each receiver. The CAT table contains the PID of the signalling message that contains the EMM. The EMM's service key is changed infrequently (e.g. every few months).
2. An ECM containing a new session key / CW is encrypted with the service key sent in an EMM. The PMT table contains the PID of the signalling message that contains the ECM. The ECM's session key / CW changes every few seconds.
3. Each video and audio stream is scrambled with the Control Word (CW).
4. If the consumer fails to pay their subscription, then a special EMM message is sent to that SC to disable it.

Examination of the above procedures shows that the fundamental weakness of DVB CA system is the reliance on an unchanging permanent key in the smart card. Specifically, attackers can have access if they manage to break the key of a single legitimate smart card. This is the reason for the fraud and the spread of counterfeit smart cards mentioned earlier.

Another fundamental weakness is the broadcast nature of the system with no feedback mechanism to exercise control except subscription payments. In other words, there is no way of knowing how many copies of a legitimate smart card are there in operation. Some operators have started using telephone lines as an ad hoc feedback mechanism.

In summary, it is very difficult to stop fraudulent cloning of smart cards in a one-way (broadcast only) DVB system without a return channel and/or an efficient way to update smart card keys. Therefore DVB CA is in need of a major upgrade and new design.

III. IP LAYER SOLUTION FOR MULTICASTING OVER SATELLTE

In this paper, we propose an IP layer multicast security solution as an alternative to the DVB-S CA system. In this solution, we use a group key management protocol call Group Secure Association Key Management Protocol (GSAKMP). GSAKMP is one of the standard key management solutions in the IETF MSEC working group [7].

This system can be used for secure satellite broadcasting services (securing MPEG streams in TV programmes and Internet multimedia streams). However the easy interworking with IPSEC makes the satellite security system more integrated with terrestrial Internet, where IPSEC is becoming widely available in routers and end systems such as Linux and Windows based workstation.

The principal actors in multicast key management are the group controller (GC) and group members (GMs). The former is responsible for creating and distributing keys and rekeying (to maintain security) as appropriate; the group members are entities with access to the group keys. The GC need not be co-located with the multicast data source. The life cycle of a GSAKMP group secure association can be divided into three phases: Group establishment, maintenance and group removal, as shown in Fig. 3 the left side of the diagram represents the actions of the GC, and the right side of the diagram represents the actions of the GMs.

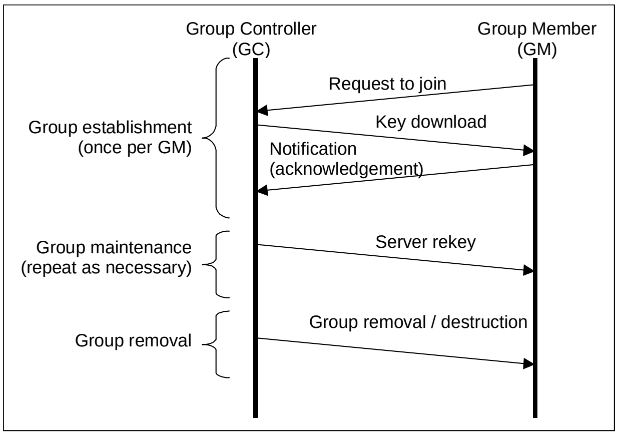
Group Controller (GC)
Group Member (GM)
Request to join
Group establishment (once per GM)
Key download
Notification (acknowledgement)
Group maintenance (repeat as necessary)
Server rekey
Group removal
Group removal / destruction

Fig. 3 GSAKMP message exchange

The multicast group may need to be rekeyed for any of a number of reasons:

(1) The group key is usually updated regularly (typically every few seconds or minutes) to reduce the probability of successful cryptanalysis of the encrypted traffic.

(2) The group key may also need to be changed on demand if it is determined that the key has been compromised.

(3) Rekeying may be required when a new member joins the multicast group. This ensures that the member cannot decrypt encoded traffic sent prior to their joining (backward secrecy).

(4) Rekeying may be required when an existing member departs from the multicast group. This ensures that the member cannot decrypt encoded traffic sent after they leave (forward secrecy).

For large multicast groups that have frequent membership changes the cost of rekeying can be significant, since satellite resources are expensive. Scalable rekeying is therefore an important problem that needs to be considered in order to support secure communications for large dynamic groups. We now consider rekey techniques for each of the four functions listed above.

Several techniques exist for rekeying (1) and (3) above: two options are for the new group key to be encrypted with either (a) the old group key, or (b) a separate “control” key negotiated during session establishment. For (2) and (4) above a different rekeying approach is required since the old key is known by at least one user who is no longer to be a recipient of the multicast transmission. We now consider options for this rekeying.

A number of multicast key management approaches have been developed with the objective of improving the scalability of group secure associations, by ensuring that parameters grow more slowly than the group size, *N*. Parameters considered include group controller encryption effort, memory requirements, network traffic, and group members’ decryption effort and memory requirements.

For large multicast groups (which can be the case for satellite services) a scalable key distribution and rekeying is essential. In this paper, we have adopted the Logical Key Hierarchy (LKH) solution as presented in RFC 2627 [7]. LKH uses a set of keys arranged in a tree structure to reduce the cost of rekeying (Fig. 4).

For a tree of outdegree k and depth d, the number of rekeys transmitted on a member compromise is reduced from $N = k^d$ (for a flat system) to $k\log_k N-1$. The system is also robust against collusion, in that no set of users together can read any message unless one of them could have read it individually.

A tree of keys is used to share a single key ‘O’ so that it is known to the GC and all GMs but to no other entities. In Fig. 4 the keys are labelled A through O, the circles again represent the pairwise keys, and the lines each represent encrypted keys sent across the network, as we shall now see. Suppose now that User 11 needs to be deleted from the multicast group. Then all of the keys held by User 11 (keys F, K, N, O) must be changed and distributed to the users who need them, without permitting User 11 to obtain them or anyone else who is not entitled to them. To do this, we must replace the keys held by User 11, proceeding from the bottom up. The seven keys sent represent a significant saving on the 16 keys that would need to be transmitted using the flat key system. We briefly write these keys as {F}12 {K}E {K}F {N}K {N}L {O}M {O}N. In general, the number of transmissions required is the sum of the degrees of the replaced nodes. In a k-ary tree of depth d, this is a total of $kd-1=k\log_k N-1$ transmissions.

GSAKMP and LKH can work with IPSEC by passing the key and the associated Security Parameter Index (SPI) that are received in the GSAKMP client (on the end system) to the IPSEC engine [7]. IPSEC can be used to secure multicast traffic as long as the SPI is uniquely identified.

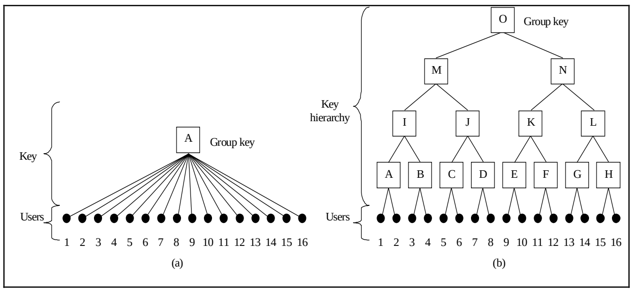

Fig. 4 Logical Key Hierarchy and flat key architectures

As an alternative to the DVB conditional access, let us consider the following scenario: A subscription based satellite broadcasting service can offer TV programmes such as movie and sports services as two separate secure multicast groups. All customers that subscribe to the movie service will be managed by the GSAKMP group controller and the movie decryption key will be distributed using LKH tree architecture. When a subscriber leaves this services, a new encryption/decryption key will be distributed through the same satellite multicast channel (for the movie service) to all remaining member except the leaving subscriber. The necessary LKH keys can distributed in a single multicast message as described in section 5. So the overheads of rekeying are low.

Within this research work the GSAKMP and LKH systems were developed and tested. Fig. 5 shows a comparison of LKH and flat key performance when rekeying is need to exclude one user from a large multicast group. The rekeying with LKH is a logarithmic function ($k\log_k N-1$) and Fig. 6 is an enlargement of the graph (the area near the origin) in Fig. 5 to show the logarithmic effect. LKH has a good scalability in the presence of the large number of multicast users. For example if there are 2048 members in a multicast group in a flat key architecture 2047 rekey messages are need to exclude a single user. In contact, using LKH only 21 rekey messages are needed (as shown in Fig. 5).

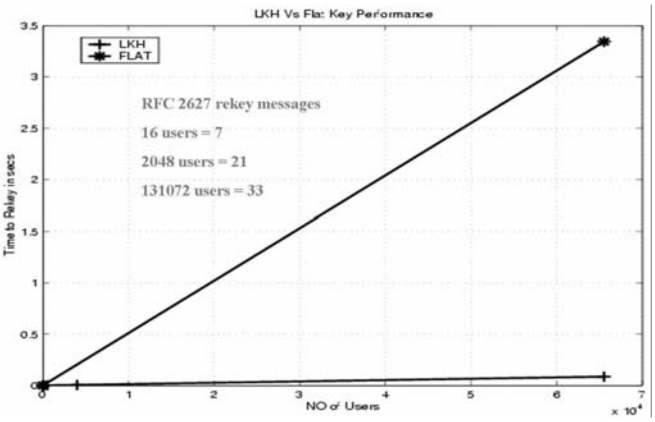

Fig. 5 Comparison of LKH with flat key architectures – large scale

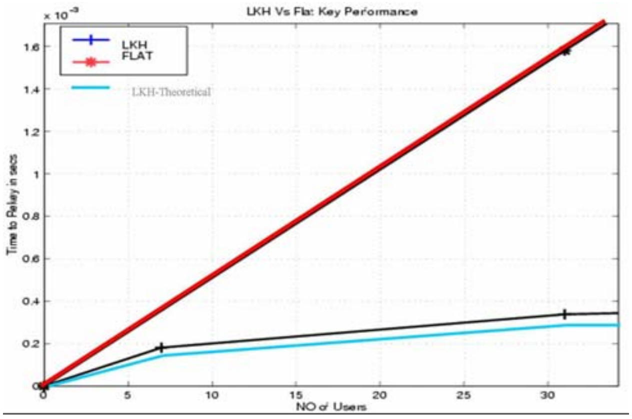

Fig. 6 Comparison of LKH with flat key architectures – small scale

IV. Conclusion

Many satellite service providers are now looking to expand their TV broadcast service offerings to include Internet services, making use of DVB standards. A key issue for the future success of these DVB systems is thus security. This paper has reviewed the DVB-S Conditional Access system and exposed its major weakness, namely one-way broadcasting system with no effective feedback channel to control fraud and misuse. An alternative solution is proposed to secure distributions (such as TV multicasting) using LKH and GSAKMP.

This solution avoids the current fraud problems related to DVB smart cards, which has an inherent weakness because the smart cards play an active role in decrypting the DVB broadcasts. The role of smart cards should be confined to subscriber authentication and storing the lowest level keys in LKH system. In this way, breaking a smart card keys will only affect that subscriber and not the whole broadcasting service. The compromised subscribers can be easily removed from the broadcast (multicast) service by a single LKH rekeying message by the GSAKMP group controller.

The GSAKMP and LKH systems had been implemented and the test result shows the good scalability of this system for large and dynamic multicast groups.

Acknowledgement

This work was supported by the EU Information Society Technologies SATLIFE project, IST-1-507675 [5] and European Space Agency (ESA) project on secure IP multicast over satellites [6].

References

[1] DVB Project home page: http://www.dvb.org
[2] U. Reimers, et al “Special Issue: Satellite Broadcasting”, International Journal of Satellite Communications, Vol. 18, No. 6, Nov.-Dec. 2000.
[3] http://www.bizjournals.com/sanjose/stories/2002/03/11/daily24.html
[4] http://www.auspaytv.com/news/2003/feb/0507.htm
[5] http:// http://www.satlife.org/
[6] http://telecom.esa.int/
[7] http://www.ietf.org
[8] ETSI, “Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt,” ETSI TS 103 197 V1.1.1 (2000-06).
[9] ETSI, “Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP Interworking over satellite IP over satellite - security aspects”, TR 102 287 (2003-11).
[10] J.M Boucqueau and X. Verians. “Next Generation Conditional Access Systems for Satellite Broadcasting," ESA Contract 16996/02/NL/US Octalis 2003.
[11] http://portal.etsi.org/dvbandca/DVB/DVBINTRO.asp