Enhanced Key Management for Cable TV Service

Yiu-Wing Leung
Department of Computer Science
Hong Kong Baptist University
Kowloon Tong, Hong Kong

Abstract
Cable TV service provider must manage the encryption/decryption keys to ensure that only the authorized set-top boxes can decrypt the pay-TV channels, and ITU recommended a key management scheme for this purpose. Nevertheless, some crackers crack and reproduce set-top boxes for profit, and many people use the pirated set-top boxes to decrypt and watch the pay-TV channels without paying subscription fee. In this paper, we enhance the key management scheme to protect the service provider’s revenue against piracy. Using the enhanced scheme, even if a cracker could crack and reproduce set-top boxes, the pirated set-top boxes are only applicable in a small geographical region (i.e., they have limited spatial applicability) and they will not function within one charging period (i.e., they have limited temporal applicability).

I. Introduction
Cable TV service provides pay-TV channels and other companions such as broadband internet access and internet telephony [1-4]. Cable TV service has been popular in some countries, and it is being developed actively in the others. For example, China has only 80 million cable TV users out of 1.3 billion people [5], and some media giants will launch cable TV service in China [6-7].

Pay-TV channels are encrypted and then broadcast from a headend to the subscribers through a cable network [1, 8]. This network has a tree-and-branch topology. In particular, the hybrid fiber-coax (HFC) network uses optical fibers for long-distance distribution and coaxial cables for local distribution (see Fig. 1) [1-2]. When the broadcast video reaches a building, it is sent to the communal broadcast cable of this building. Each subscriber is provided a set-top box to receive and decrypt the pay-TV channels [1, 8].

If a subscriber has paid the subscription fee for a channel in a charging period, his set-top box can decrypt this channel in this charging period; otherwise, it cannot. For this purpose, ITU recommended a scheme to manage the encryption/decryption keys [9-10] (this scheme is described in section II). Using this scheme, a vital key called private key \( PK_s \) to set-top box \( s \). This key is stored in a smart card of this set-top box. This research is supported by the Hong Kong Research Grant Council.

II. Review of ITU Key Management Scheme
ITU recommended the following scheme to manage the encryption/decryption keys for cable TV service:

1. The service provider assigns a distinct private key \( PK_s \) to set-top box \( s \). This key is stored in a smart card of this set-top box.

2. The service provider selects an authorization key \( AK_c \) for channel \( c \), and changes this key at least once per charging period. If subscriber \( s \) has paid the subscription fee for channel \( c \) in a charging period, the service provider delivers \( AK_c \) to set-top box \( s \).
box $s$ in order to authorize this set-top box to decrypt channel $c$. Since a cable network uses a broadcast medium, this delivery is done securely as follows:

- The service provider uses the private key $PK_s$ to encrypt $AK_c$ to produce $PK_s(AK_c)$ (where $K(I)$ denotes the item encrypted by the key $K$). Then the service provider broadcasts $PK_s(AK_c)$ over the cable network.
- Set-top box $s$ receives and decrypts $PK_s(AX_c)$ to get $AK_c$. The other set-top boxes cannot decrypt $PK_s(AX_c)$ to get $AK_c$, because they do not have the private key $PK_s$.

3. The service provider uses a scrambling key $SK_c$ to encrypt the video of channel $c$, where $SK_c$ is changed frequently (say, once per minute). It broadcasts $SK_c$ (video of channel $c$) and $AK_c(AX_c)$ over the cable network.

4. When an authorized set-top box is tuned to channel $c$, it receives $AK_c(AX_c)$ and $SK_c$ (video of channel $c$). It uses $AK_c$ to decrypt $AK_c(AX_c)$ to get $SK_c$, and uses $SK_c$ to decrypt $SK_c$ (video of channel $c$) to recover the video of channel $c$.

In a recent study [10], Tu, Laih and Tung reduced the communication overhead in the above scheme. They exploited the broadcast nature of the cable networks, and used an additional type of keys to distribute the new authorization keys efficiently.

### III. Enhanced Key Management

#### A. Main Ideas

We enhance the ITU key management scheme to protect the service provider’s revenue against piracy. Our main ideas are as follows:

1. We divide a cable network into multiple regions and use different authorization keys in different regions. It is likely that a cracker could only access a limited number of authorized set-top boxes and a small part of the cable network (e.g., he could only access his own set-top box and a network branch in his apartment). Therefore, he could hardly obtain sufficient information to find out the network division and crack all the authorization keys. As a result, the pirated set-top boxes have limited spatial applicability.

2. It is likely that a subscriber of cable TV service has also subscribed to the traditional telephony service with a unique telephone number. To change the authorization keys (e.g., for a new charging period), the service provider uses a point-to-point telephone channel to deliver the new encrypted keys to each authorized set-top box automatically (i.e., it avoids broadcasting the new encrypted keys over the cable network). In this manner, the pirated set-top boxes can hardly intercept these new keys from the point-to-point telephone channels. As a result, the pirated set-top boxes have limited temporal applicability.

#### B. Enhanced Key Management

We realize our first idea as follows. We divide the cable network into multiple regions, and adopt a distinct authorization key $AK_{r,c}$ for channel $c$ in region $r$. For this purpose, we equip a cryptographic module beside the amplifier in each region (e.g., see Fig. 2). In region $r$, the cryptographic module receives the scrambling key $SK_c$ from the headend securely and encrypts it to $AK_{r,c}(SK_c)$ for this region.

![Fig. 2: A cable network is divided into multiple regions where different regions adopt different authorization keys. In each region, a cryptographic module is equipped beside the amplifier, and it uses a distinct authorization key to encrypt the scrambling keys for this region.](image-url)
If subscriber \( s \) in region \( r \) has paid the subscription fee for channel \( c \) in a charging period, his set-top box receives \( PK_r(\text{AK}_r,c) \) automatically through its modem and telephone channel. This set-top box decrypts \( PK_r(\text{AK}_r,c) \) to get \( \text{AK}_r,c \). When it is tuned to channel \( c \), it receives \( \text{AK}_r,c(SK) \) and \( SK(\text{video of channel} \ c) \) from the cable network. It uses \( \text{AK}_r,c \) to decrypt \( \text{AK}_r,c(SK) \) to get \( SK_r \), and then uses \( SK_r \) to decrypt \( SK_r(\text{video of channel} \ c) \) to recover the video of channel \( c \).

C. Reducing the Impact of Piracy

The enhanced key management scheme can reduce the impact of piracy on the service provider’s revenue as follows.

*Pirated set-top boxes have limited spatial applicability*

It is likely that the cracker could only access a small part of the cable network and a limited number of authorized set-top boxes (e.g., he could only access his own set-top box and a network branch in his apartment). Thus, he could hardly obtain sufficient information to find out the network division and crack all the authorization keys for all the regions. This leads to two desirable consequences:

1. Even if the cracker could crack and reproduce a set-top box, the pirated set-top boxes are only applicable in one region. This can reduce the impact of piracy on the service provider’s revenue, especially when the cable network is divided into more regions.

2. The cracker does not know the exact boundary of each region, so he would have difficulty to sell the pirated set-top boxes to the general public. This can reduce the impact of piracy on the service provider’s revenue.

*Pirated set-top boxes have limited temporal applicability*

To change the authorization keys (e.g., for a new charging period), the service provider encrypts the new keys and delivers them to each authorized set-top box in advance through a point-to-point telephone channel. In this manner, the pirated set-top boxes can hardly intercept these new keys. As a result, when the current authorization keys expire within one charging period, the pirated set-top boxes will not function.

If the cracker attempts to crack and provide the new authorization keys to the pirated users regularly, he would have a large overhead and a risk of being traced, identified and arrested. On the other hand, the pirated users may also be unwilling to provide their contact information (such as telephone numbers) to the cracker for fear of being identified and prosecuted.

Flexible Security Control

If a district has a larger risk of piracy (e.g., its residents have relatively low income), the service provider can execute a tighter security control on this district as follows. It divides this district into more regions and changes the authorization keys for these regions more frequently and aperiodically. As a result, the cracker would encounter a larger difficulty and has a larger overhead to: (i) find out all the regions of this district, (ii) monitor the change of authorization keys in each region, and (iii) crack all the new authorization keys. Consequently, the service provider can reduce the risk of piracy in this district.

D. Cost and Overhead

The enhanced key management scheme involves the following cost and overhead:

- **Cost:** Modems are needed for automatic delivery of updated authorization keys. Nowadays the cost of a modem is very low. In addition, a cryptographic module is needed in each region for encrypting the scrambling key. A scrambling key is not long (say, it has 128 bits), so a cryptographic module can be a low-cost computer to do this encryption.

- **Overhead in the planning phase:** It is necessary to record the network branches belonging to each region and install a cryptographic module beside the amplifier in each region (e.g., see Fig. 2). These are done only once, and the overhead is small.

- **Overhead in the operation phase:** It is necessary to record the telephone numbers of the subscribers for automatic delivery of updated authorization keys. This overhead is very small.

The above cost and overhead are small, and we believe they are worthy for protecting the service provider’s revenue against piracy.

E. Number of Modems Required

The service provider changes the authorization keys at least once per charging period, and it uses a pool of \( N \) modems to deliver the new keys to the authorized set-top boxes before the effective date. In the following, we determine \( N \) to ensure complete delivery before the effective date.

Suppose the current authorization keys will be used for a duration of \( T \). In this duration, the service provider delivers the new authorization keys to the authorized set-top boxes, and these keys will be used on the effective date when the current ones expire. Let \( S \) be the number of authorized set-top boxes, and \( \tau \) be the time required to deliver the authorizations keys to set-top box \( s \). \( \tau \) is a random variable as it depends on various probabilistic factors such as re-dialling and retransmission, and its mean \( \bar{\tau} \) and standard deviation \( \sigma \) can be measured experimentally. The time required to deliver the new authorization keys to all the set-top boxes is \( \Sigma_{s=1}^{S} \tau_s \). The available time for delivery before the effective date is \( T \), and there are \( N \) modems for simultaneous
delivery (where \( N \) is usually much smaller than \( S \)). Therefore, the probability \( \zeta \) of complete delivery before the effective date is given by \( P \left( \sum_{i=1}^{n} \tau_i \leq NT \right) \).

Since \( S \) is very large in practice and \( \tau_1, \tau_2, \ldots, \tau_n \) are independent and identically distributed, we apply the central limit theorem \([18]\) to accurately approximate

\[
\zeta = P \left( Z \leq \frac{NT - \bar{S}}{\sqrt{S \sigma^2}} \right)
\]

where \( Z \) is a unit normal random variable. We determine \( N \) to ensure that the probability \( \zeta \) of complete delivery before the effective date is at least \( 0.9999 \) where \( \zeta \) is a given requirement (e.g., determine \( N \) such that \( \zeta \geq 0.9999 \)).

**Example 1**

Suppose the authorization keys are changed once per week, \( \tau = 100 \) seconds, \( \sigma = 20 \) seconds, and \( \bar{S} = 0.9999 \). To ensure that the probability of complete delivery before the effective date is at least 0.9999, Table 1 shows the number of modems required \( N \) for different number of set-top boxes \( S \).

**Table 1:** Number of modems required for different number of set-top boxes in Example 1.

<table>
<thead>
<tr>
<th>Number of set-top boxes ( S )</th>
<th>Number of modems required ( N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>100,000</td>
<td>17</td>
</tr>
<tr>
<td>200,000</td>
<td>34</td>
</tr>
<tr>
<td>300,000</td>
<td>50</td>
</tr>
<tr>
<td>400,000</td>
<td>67</td>
</tr>
<tr>
<td>500,000</td>
<td>83</td>
</tr>
<tr>
<td>600,000</td>
<td>100</td>
</tr>
<tr>
<td>700,000</td>
<td>116</td>
</tr>
<tr>
<td>800,000</td>
<td>133</td>
</tr>
<tr>
<td>900,000</td>
<td>149</td>
</tr>
<tr>
<td>1,000,000</td>
<td>166</td>
</tr>
</tbody>
</table>

**IV. Conclusions**

We enhanced the key management scheme for cable TV service to protect the service provider’s revenue against piracy. Using the enhanced scheme, even if a cracker could crack and reproduce set-top boxes, the pirated set-top boxes have limited spatial and temporal applicability. The enhanced scheme is also flexible as it can execute a tighter security control on those districts with a larger risk of piracy.

**References**


