

REPORT ITU-R BT.2052*

**Protection of end-users' privacy in
interactive broadcasting systems**

(Question ITU-R 111/6)

(2005)

1 Introduction

Interactive broadcasting systems enable attractive services to end-users. On the other hand, the system offers the opportunity to collect information related to the end-user to the service provider or the other third party or parties, and to send a malicious program code to the receiver to malicious party or parties. To protect end-users' privacy from potential threat, information to be protected and potential attack points in the interactive broadcast chain should be clarified. In this Report, a detailed analysis of interactive broadcast systems is discussed with two principles below to clarify the problem of protection of end-users' privacy:

- Free-to-air broadcasting services, even when including interactive elements, should be available to the end-users without any need for a return channel connection.
- Any information of a personal nature is, by default, considered private.

A privacy threat to a broadcast receiver with a return channel can potentially materialize as soon as a connection to a remote computer is established over the return channel.

2 Information to be protected

Considering the second principle in the previous section, all data related to the user should be regarded as potentially sensitive. There are different kinds of user data such as:

- personal data, e.g. name, date of birth, personal profiles and preferences;
- link data, e.g. address and telephone number, bank account or credit card number;
- data stored within the broadcast receiver, e.g. zapping history, return/interaction channel usage history, ID number;
- data stored outside the broadcast receiver, for a static receiver, e.g. return/interaction channel usage history, for a mobile receiver, e.g. location data.

This tells that protection of the end-user's privacy can be achieved when all the elements affecting it in the interactive broadcast chain work properly.

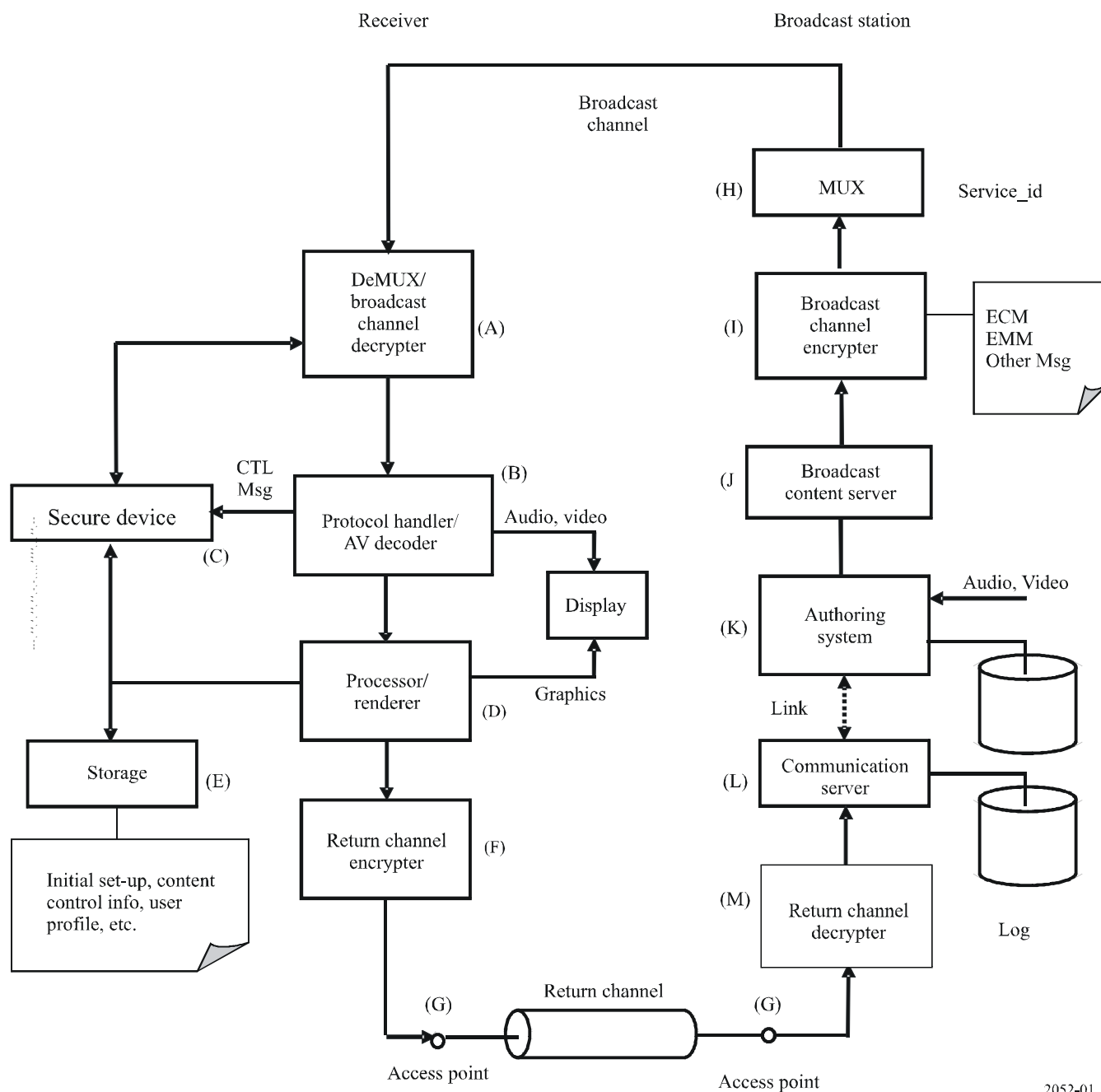
3 Interactive broadcast system model

In order to approach these questions, an analysis of threat to privacy infliction should be undertaken. Typical models for the interactive broadcast chain, with a unidirectional and bidirectional return channel, as illustrated in Figs. 1 and 2 respectively, are used for this analysis.

* This Report is brought to the attention of ITU-T SG 9, ITU-T SG 17 and ITU-D SG 2.

FIGURE 1

Model for an interactive broadcast chain with a unidirectional return channel



2052-01

The receiver in Fig. 1 comprises the following components:

(A) *DeMUX/broadcast channel decrypter*

This is to descramble a broadcast signal that has been encrypted for certain purposes such as pay-service or copy control of the broadcast content.

- (B) *Protocol handler/AV decoder*
This is to handle various broadcast protocols such as transport stream and carousel, etc. in a receiver and audio/video decoding. Data or messages other than audio/video signals taken out of the received signal by this are passed to an appropriate part of subsequent processes.
- (C) *Secure device*
This stores an end-user's authorization information, including identification of the user and key(s) for descramble. Certification authority can track the end-user's name, address and telephone number, etc., through the identification number.
- (D) *Processor/renderer*
This controls receiver behaviour instructed by both a broadcast content and a system program.
- (E) *Storage*
This keeps information provided by the broadcast content, initial set-up, or user. Information provided by a user includes user profile such as name, age, sex, address, genre of interest of contents, etc.
- (F) *Return channel encrypter*
This enciphers message(s) sent through a return channel. This could be optional.
- (G) *Access point*
A point to connect a receiver to a communication network for return channel. To access the network, a receiver may require information to logon the network, e.g. user-id and password, or number to dial.

A broadcast station provides the following components:

- (H) *Multiplexer*
This combines broadcast services into a single stream and provides signalling information such as PSI/SI. Service_id of each service is included in SI.
- (I) *Broadcast channel encrypter*
This enciphers broadcast contents and provides key(s) information and control message(s) for a descrambler in a receiver.
- (J) *Broadcast content server*
This feeds broadcast contents to a broadcast channel encrypter (I).
- (K) *Authoring system*
Interactive contents are authored by this system. Some contents may be renewed frequently to reflect end-user response derived from a communication server to the content.
- (L) *Communication server*
This gathers responses of end-users. One possible use of these responses is to update the content. Gathered information or communication log may be stored if needed.
- (M) *Return channel decrypter*
This decipheres incoming encrypted messages from receivers through return channel. This is a counterpart of encrypter provided in a receiver.