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

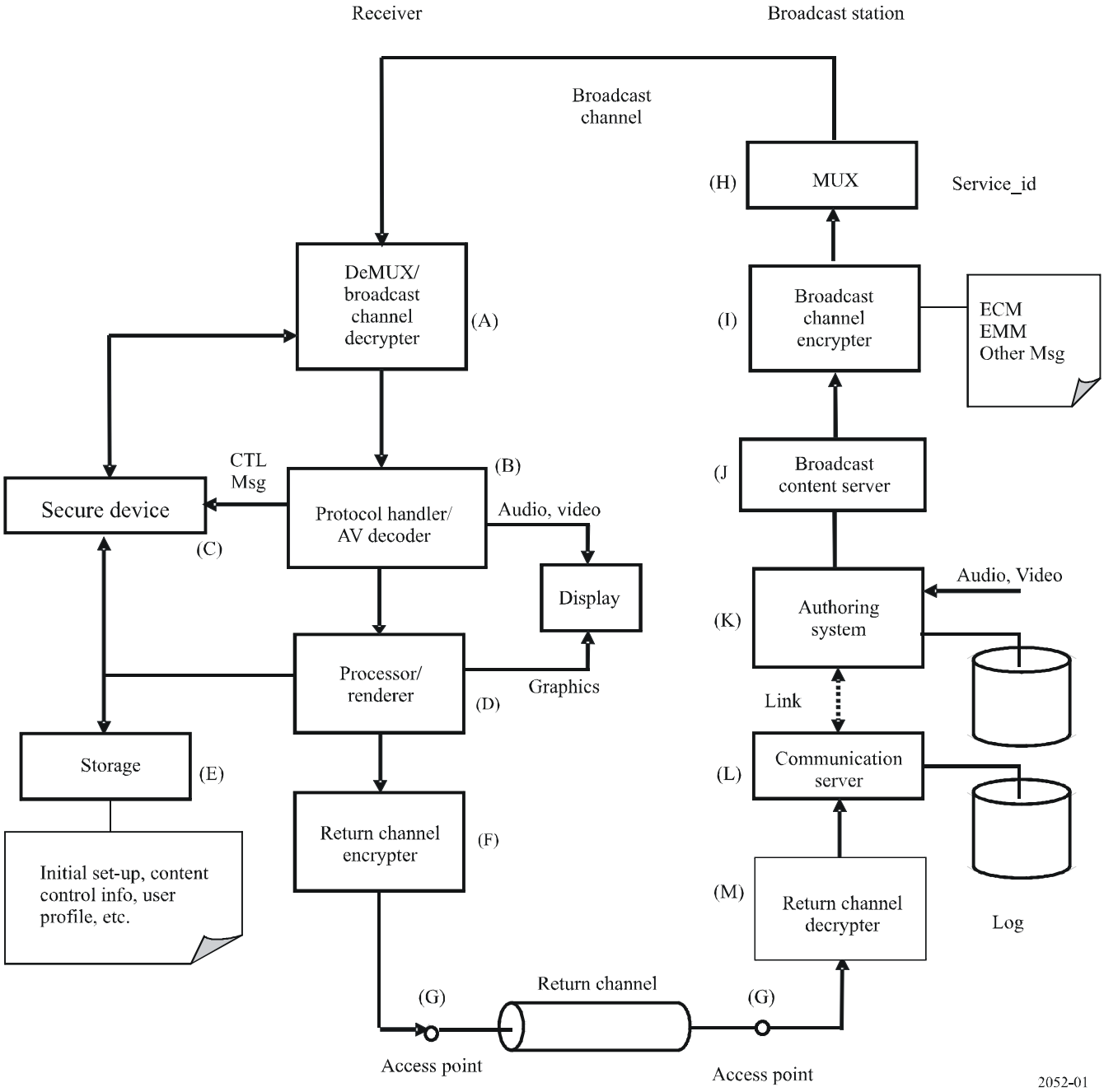
In order to approach these questions, an analysis of threat to privacy infliction should be undertaken. Typical models for the interactive broadcast chain, with a unidirectional and bidirectional return channel, as illustrated in Figs. 1 and 2 respectively, are used for this analysis.

---

* 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



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*

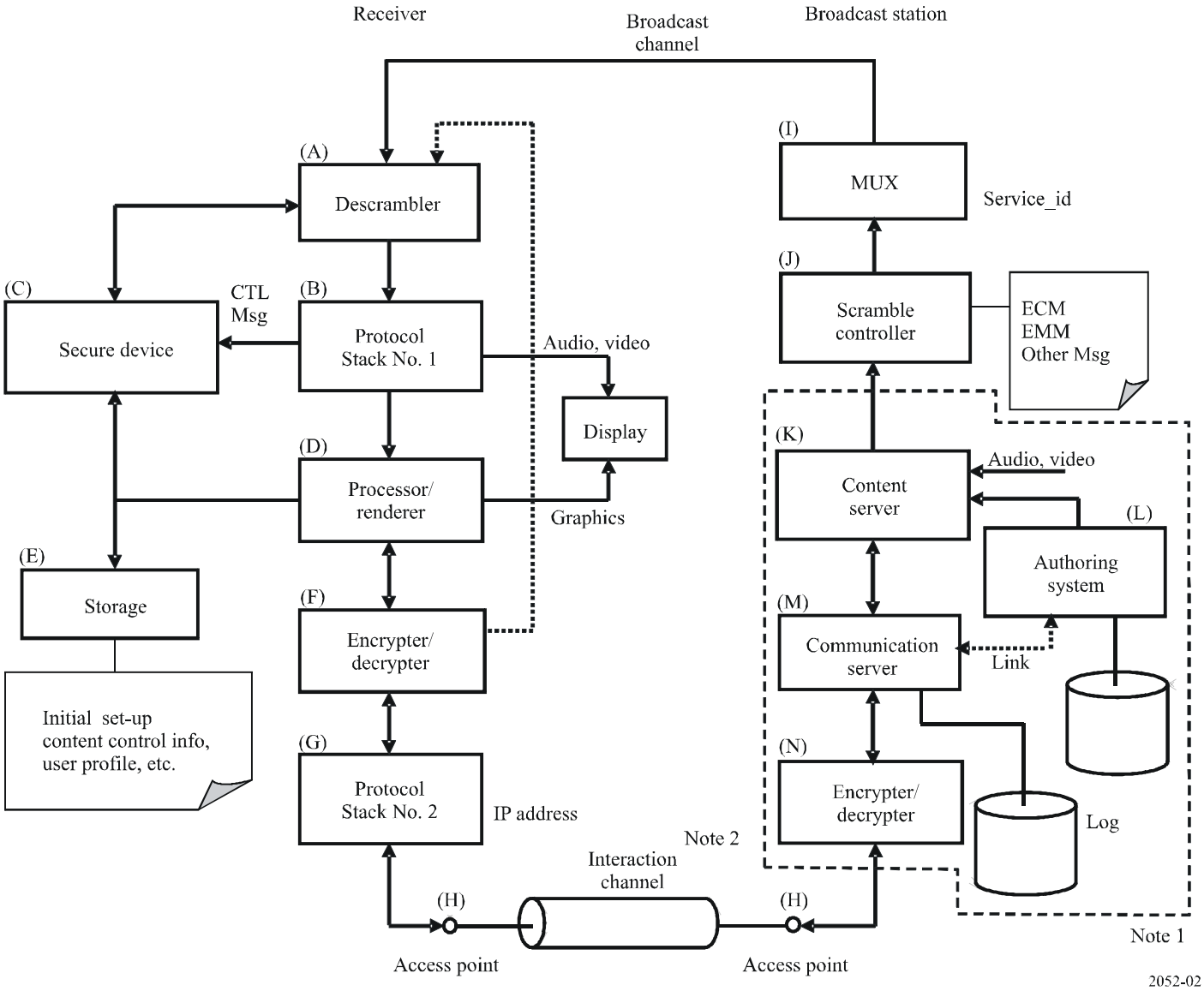
This gathers responses of end-users. One possible use of these responses is to update the content. Gathered information or communication log may be stored if needed.

(M) *Return channel decrypter*

This deciphers incoming encrypted messages from receivers through return channel. This is a counterpart of encrypter provided in a receiver.

FIGURE 2

Model for an interactive broadcast chain with a bidirectional return channel



NOTE 1 – Multiple content providers using content server (K), authoring system (L), communication server (M) and encrypter/decrypter (N) or part of them may take part in establishing the interactive broadcast service. For example, additional audio/visual component fed through interaction channel is provided by a different provider from broadcaster. The actual structure of these components above depends upon the service.

NOTE 2 – The destination at provider side, i.e. broadcaster side, of the interaction channel depends upon the structure described in Note 1.

A receiver in Fig. 2 comprises the following components:

(A) *Descrambler*

This is to descramble a signal that has been encrypted. In some cases, an encrypted signal may come from the interaction channel in addition to the broadcast channel.

(B) Protocol stack No. 1

This is to handle various broadcast protocols such as transport stream and carousel, etc. in a receiver. Data or messages taken out of a received signal by this are passed to an appropriate part of subsequent processes.

(C) *Secure device*

This stores information regarding legality of an end-user to enjoy the services, 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 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. Information provided by the content may be some tags to hold a state of the content, or to distinguish each receiver or user.

(F) *Encrypter/decrypter*

This enciphers and deciphers a signal sent and received through the interaction channel. This may not always be employed to all kinds of interaction channel. Authentication of the content from interaction channel may be applied here when using a different technique from authentication for broadcast channel applied with secure device (C). If the protocol in the interaction channel used to deliver a content to a receiver is the same as that in the broadcast channel, a received signal will be forwarded to the descrambler (A).

(G) *Protocol Stack No. 2*

This handles communication protocol used for the interaction channel. In case of Internet protocol, this holds the IP address.

(H) *Access point*

A point to connect a receiver to a communication network for the interaction channel. Physical connection to the access point varies by the interaction channel medium; telephone line for dial-up connection, Ethernet for broadband connection and base station for wireless connection including WiFi and cell phone network.

A broadcast station comprises the following components:

(I) *Multiplexer (MUX)*

This combines broadcast services for broadcast channel into a single stream and provides signalling information such as PSI/SI. Service_id of each service is included in SI.

(J) *Scramble controller*

This scrambles broadcast contents for broadcast channel and provides key(s) information and control message(s) for the descrambler (A) in a receiver.

(K) *Content server*

This routes components of the content such as data broadcast content, video or audio for transmission toward a receiver. When this receives a trigger or a request for transmission based on program timetable, all the components of the content at that time will be routed to the broadcast channel.

When a request message for transmission comes through the interaction channel, requested component(s) of the content will be routed to the interaction channel. Selection of the components follows an incoming request message from the interaction channel, which is generated by the instruction of the content running on processor/browser (D) in a receiver, or by a system program of the receiver.

(L) *Authoring system*

Interactive content is authored by this system. Some content may be renewed frequently to reflect end-user responses, or instantly created ("active content") based on information of a sender of an incoming request message from the interaction channel derived from the communication server (M).

(M) *Communication server (M)*

This controls all the communication on the interaction channel including the establishment of logical connection, transmission/reception of messages and logical disconnection. A typical example is a web server. This can gather end-users' responses to the content as well.

(N) *Encrypter/decrypter (N)*

This enciphers and deciphers messages for the interaction channel. This is a counterpart of encrypter/decrypter (F) in a receiver.

4 Consideration on personal information and its handling in the elements of the interactive broadcast chain

Based on the two models described in the previous section, generated or stored information related to the end-user's privacy and potential threat to it as a result of the process of the information is discussed below.

4.1 Receiver

A receiver is a major source of private information in an interactive broadcast chain. Following information are examples kept in a secure device and/or storage, or created by a processor as a result of user interaction:

– Viewing history
– Return/interaction channel usage
– History of interactive operation
– Personal profiles and preferences
– ID number.

In some interactive broadcast systems, the ID number is used for the purpose of content copy control even in free-to-air services.

4.2 Return channel

The following aspects of return channel characteristics and configuration are to be considered:

4.2.1 Return channel characteristic

– *Non-disclosure of the channel specification*

This may help to protect the system including the end-user's receiver from attack by malicious third party or parties.

– *Communication operator*

In the case of employing IP in the interaction channel, protection of the DNS server may be one of the key actions to protect the end-user's receiver from attack by malicious third party or parties.

– *IP address*

In general, a dynamic assignment of IP address (DHCP) by the Internet service provider (ISP) makes it difficult for the entity who owns a server to find out the relationship between IP address and personal information. But if the interaction channel is a broadband IP connection, the channel may be shared with other equipment, such as PCs using a broadband router. In the case of using the router, a connection is established at all times and this may lead to keeping the same IP address even in a DHCP environment. This degrades anonymity of the end-user to the broadcaster. Improvement of anonymity of the end-user can be achieved by using a trustworthy proxy that has no relationship to the content author/service provider.

4.2.2 Return channel configuration

– *Telephone number of a caller*

In the case of using a telephone line for return channel, notifying this number to the destination leads to giving an opportunity to the service or content provider to collect information about who responds to it.

– *Network configuration for broadband IP connection*

In the case of using a broadband IP communication network such as DSL, optical fibre and WiFi, the gateway device at the access point should be configured properly. If a broadband router installed near the receiver is not configured properly, this may be a possible hole to probe the activity of return channel communication. If a WiFi channel is not configured securely enough, attackers will monitor the traffic and obtain important parameters such as the nearest DNS server address. This may result in a takeover of the DNS server and a fake DNS server will subsequently lead the connection to the improper server.

4.3 Content/service provider

The following aspects are to be taken into account concerning the information exchange between the content/service provider and the receiver:

– *Authentication*

When transmitting information from the receiver to the content author/service provider, authentication carried out by the receiver is important to prevent the establishment of a connection to a fake server. Such a server is considered malicious, thus transmitted information will be monitored, stored and consumed for unintended purpose by the malicious party or parties. The seriousness of this attack depends on the choice of return channel; an IP connection is considered more vulnerable than a direct connection to such a server using a telephone line.

In the bidirectional return channel model illustrated in Fig. 2, the communication server (M) should be authenticated properly by a receiver when the interaction channel is used as a “forward” channel. Authentication of a receiver may also be needed with the same reason why a scramble controller (J) and descrambler (A) pair is used. Without the authentication of communication server (M), a malicious code can be transmitted to the receiver by pretence. In other words, a fake server will deliver a malicious code to the receiver. A takeover of DNS (Domain Name System) server near the receiver makes this activity possible. The encrypter/decrypter pair (F) and (N) is in charge of authentication in the interaction channel. When using the same authentication technique of the broadcast channel, an incoming signal from the interaction channel should be forwarded to the descrambler (A).

– *IP address*

In general, a communication using IP often makes a record of access in a server, e.g. access log. In Fig. 1, the communication server (M) is in charge of it. This keeps the date, time and IP address of an entity that has made a connection and, in some cases, the file name that has been retrieved by the entity.

– *Agreement of a viewer for the transmission of information related to the viewer*

The request for agreement to transmit information related to the viewer to the content/service providers or any third party or parties requires the end-user's understanding of how the interactive broadcast system works. A too-simplified instruction for this agreement may mislead the viewer's intention. Furthermore, some mechanism is needed to catch up with the change of the service or the viewer's intention for a one-time agreement to the specific service or content/service provider. On the other hand, a request for the agreement for transmission of information to the content author/service provider or any third party or parties at each time of transmission may bother the end-user, thus the end-user will not care about the warning or request in this case. Consequently, the provider offers the option for general acceptance on the basis of stored user profiles. In this case, careful design of the memory, where to save and how to access such information, is needed.

5 Privacy policy and its implementation

Privacy policy is the primary rule or guideline determined by the service provider as to how the end-user's privacy should be treated in the interactive broadcast service. Privacy policy is determined by many aspects; cultural background, regulations, service usability, content protection requirements, etc. Any technical method for the protection of end-users' privacy corresponds to tools to implement the policy.

Possible approaches for the implementation are as follows:

a) *Toolset approach*

This approach provides a list of tools to protect the end-user's privacy at a relevant function in the interactive broadcast chain. The provider has to choose appropriate tools among the list for each element in the chain in order to satisfy the established privacy policy. Choice of SSL (Secure Socket Layer) for protocol stack No. 2 (G) and encrypter/decrypter (N), and Smart Card for secure device (C) in Fig. 2 is one example to this approach.

b) *Multisystem approach*

This approach provides several sets of tools that cover the entire interactive broadcast chain. For example, set 1 comprises Tool A for scramble controller (J) and descrambler (A), Tool B for secure device (C), and Tool C at communication server (M) in Fig. 2. Each set of tools represents a certain privacy policy.

In both cases, available tools for each element in the chain vary in accordance with the elements used.

In the case of controlling the transmission of private information by the end-user, the following are examples of interaction behaviour between the end-user and the receiver as determined by the established policy:

– No automatic connection to return/interaction channel by default.

– Connection to the interaction channel is established by end-user action only.

– The end-user should have the opportunity of knowing what information is going to be transmitted.

– No transmission of any data related to the end-user should take place without the end-user's consent.

Considering that the receiver is under the control of both its pre-installed system software and the interactive content, some of the behaviours listed above will be accomplished by the cooperation of the receiver and the other elements comprising the service.

6 Other aspects for end-users' privacy protection

In addition to the analysis described above, to provide highly secure privacy protection for interactive broadcast services to the end-user, further consideration is needed on the following matters, which other technical elements for the services are tied to:

– Trade-off to maintain usability of interactive broadcasting services, while maintaining the anonymity of the end-user.

– Trade-off for the conflict between privacy protection and content protection.

– Development of techniques and systems that allow for future evolution.

7 Conclusion

In this Report, information regarding the end-user, how it propagates and is processed in the interactive broadcast chain and protection against the theft of information or acquisition of malicious program by the third party are discussed. The creation of a Recommendation regarding privacy protection should take into account the system analysis in this Report.