9

An integrated solution for secure communications over B-ISDN

J. Forné, J. L. Melús
Department of Applied Mathematics and Telematics
UNIVERSITAT POLITECNICA DE CATALUNYA
Gran Capitan s/n. Módul C3. Campus Nord. Barcelona (SPAIN)
Voice: +3434016011; Fax: +3434015981
email: {teljfm, teljmm}@mat.upc.es

Abstract

The Broadband Integrated Services Digital Network (B-ISDN) is expected to be the public communications network of the future. One of the prime factors influencing the development of such a network is the emergence of a large number of teleservices with different requirements (sometimes still unknown). However, a common requirement for all these services is the need to be protected against unauthorised use, which can be achieved through a suitable security system.

Although specific security mechanisms can be developed for each application and service on the network, we consider that an integrated solution providing security services for all types of multimedia applications is more efficient. Therefore, we study the integration of the different security services in the network architecture, comparing different possibilities and proposing an integrated solution where bulk encryption is placed on top of the ATM Adaptation Layer (AAL).

Keywords

B-ISDN, ATM, network security, security services

1 INTRODUCTION

In recent years, technological advances in the areas of VLSI, packet switching technology and fiber optic communications have made possible the development of a high speed integrated services network which can carry all fundamental media streams: data, voice and video. Such

P. Horster (ed.), *Communications and Multimedia Security II*

a network has been named B-ISDN (Broadband Integrated Services Digital Network), and the Asynchronous Transfer Mode (ATM) has been adopted by the CCITT as a universal transfer mode for B-ISDN (CCITT I.121, 1991). This transfer mode is based on the segmentation of the information stream into fixed-length packets (called cells). These cells are transferred asynchronously according to the source demand. The ATM is essentially a connection-oriented technique. All the characteristics of the service are negotiated between the user and the network during the connection establishment period and all information is routed using a virtual circuit assigned for the complete duration of the connection. The routing information is written in the header of each cell and consists of a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI).

The protocol architecture for B-ISDN is defined by (CCITT I.321, 1991). Two layers of the B-ISDN protocol architecture relate to ATM functions. There is an ATM layer common to all services, which provides packet transfer capabilities, and an ATM adaptation layer (AAL), which is service-dependent. The AAL maps higher-layer information into ATM cells to be transported over B-ISDN, then collects information from ATM cells for delivery to higher layers. The use of ATM creates the need for an adaptation layer to support information transfer protocols not based on ATM. The protocol reference model makes reference to three separate planes: the user plane, the control plane and the management plane.

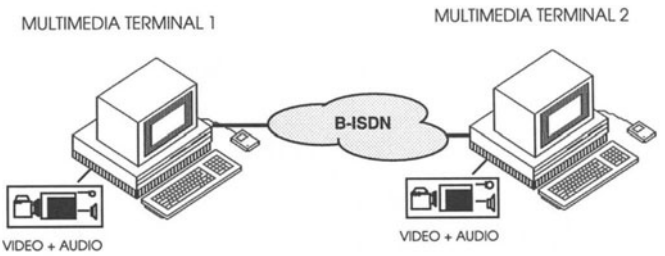

Figure 1 Scenario A: multimedia terminals directly connected to the B-ISDN.

Although terminals supporting only voice or data can be connected to the B-ISDN, multimedia terminals are expected to be the physical support by means of which data, voice and video services will access the broadband network. Figure 1 shows two multimedia terminals that communicate through the ATM network. Each terminal must have a suitable interface for video and audio applications, as well as an interface for the broadband network.

The scenario presented in Figure 1 will be very usual in the future B-ISDN, where a great range of services will be supported. Most of these broadband services will also require some security services, like confidentiality, integrity, authentication, access control and nonrepudiation. To implement these security services, security mechanisms (like encryption and key management) must be used. In this paper we will present some of the requirements for a system to make the broadband network secure. Subsequently, we will study the placement of the security services and the related security mechanisms within the ATM layered protocol.

Although we want to secure multimedia terminals communicating through the broadband network, as presented in Scenario A, we cannot forget that an interconnection scenario such

as Scenario B will be very usual, especially during the initial periods, when many users will use the network for LAN and MAN interconnection. In Figure 2 such a scenario is illustrated. We can see that multimedia terminals MT1 and MT2 directly access the broadband network, MT3 access through a Local Area Network, MT4 through a Metropolitan Area Network, and MT5 through a LAN interconnected to the B-ISDN via a MAN. The solution we will propose for Scenario A should coexist with the interconnected Scenario B.

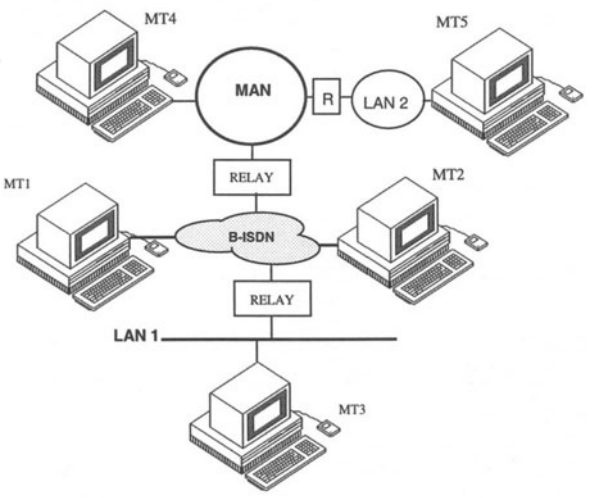

Figure 2 Scenario B: Some terminals are directly connected to the B-ISDN, while others access it through LANs and MANs.

Previous related work

We firstly faced the problem of making communications over the B-ISDN secure as a result of our work in the CRIPTO project (Forné et al., 1995), belonging to the Spanish Broadband Program (PLANBA). The CRIPTO project was set to provide secure communications between multimedia terminals communicating over the testbed PLANBA broadband network, called RECIBA (Martínez and Fernández-Amigo, 1993).

The placement of the security services within the ATM Protocol Reference Model is of great importance in order to provide them to the applications at the lowest possible cost. In the CRIPTO project the specific architecture of the multimedia terminal, which is unlikely to be repeated, forced us to place the encryption mechanisms between the ATM and the AAL layers, as shown in option c of Figure 4. Unfortunately, this choice imposes very strong requirements for the ciphering device, as will be mentioned in Section 3.

Next we consider the problem of securing communications over the B-ISDN without restrictions due to particular architectures of multimedia terminals. We will specifically study some options for placing the encryption mechanism, and we will finally choose to place it above the ATM Adaptation Layer (AAL). Operating in this way, we will provide a seamless

Secure AAL (SEC-AAL) for the higher layer protocols that will provide security services for the multimedia applications.

2 REQUIREMENTS FOR THE SECURITY SYSTEM

The following are the requirements for the security system:

1.- The security system must provide security services only for sensitive applications

There is no sense in encrypting all unclassified information. Moreover, the requirements of different applications vary greatly. While authentication and integrity are essential for applications like electronic commerce, other applications would require confidentiality or non-repudiation. To provide all security services for every application would be very difficult and inefficient, and the cost would be very high. This means that the security system should have a suitable application interface (API) to let the application demand the required security services.

2.- The session key used for the bulk of the information must depend on the application

Different applications may require different security services and different levels of security. Furthermore, they could require a different Quality of Service (QoS), i. e., different cell-loss ratio, different cell delay or cell-delay variation, etc. If we cho0se the session key depending upon the end multimedia terminals, the sequence of the information belonging to different applications could not be preserved, making decryption impossible. If we try to recover the order buffering the information of the different channels (in the hypothetical case that this were possible, this would depend on the layer in which encryption was done), then delays, delay variations and other QoS parameters will be expanded from one channel to the others, making the coexistence of different QoS impossible. From our point of view, security is another QoS parameter and security aspects should be included during the connection establishment period in the B-ISDN signalling framework.

3.- The encryption mechanism must provide fast encryption for the bulk of the information

Obviously, B-ISDN is a high speed network and fast encryption is necessary in order to guarantee confidentiality and integrity in bulk high-speed sensitive applications. This forces the use of symmetric algorithms to encrypt large quantities of data. Nowadays, stream ciphers [RUEP] seem to be the best option for fast implementation of these two services, where the ciphertext is obtained by combining (by addition at Module 2) the plaintext with a pseudo random (PN) sequence. In the receiver the same process (using the same PN sequences) must be applied.

Since multimedia applications requiring up to tens and even hundreds of Mbps are not far off, hardware implementations of stream ciphers are necessary in order to provide the services of confidentiality and integrity for these broadband applications. This can be achieved with a growable structure that permits the generation of several independent pseudo

random bits each time, allowing faster encryption as higher-speed multimedia applications and terminals appear (Cruselles et al., 1995). Another example of fast hardware stream cipher was the ASIC developed for the CRIPTO project (Guía de la et al., 1994).

Nevertheless, asymmetric algorithms (public key cryptography) can be used for applications that do not require a high bandwidth to provide specific services such as nonrepudiation. Public key cryptosystems are also very useful for authentication and key management, where the encryption speed is not essential.

4.- Data compression must be performed before encryption and encryption must be performed before channel coding

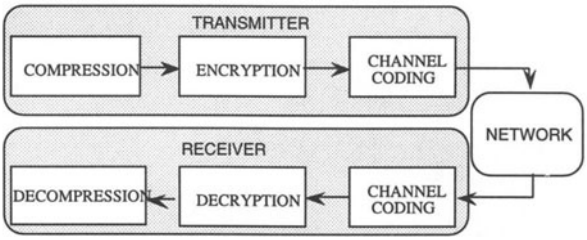

Figure 3 Order of compression, encryption and channel coding at the transmitter and the receiver.

Data encryption before compression would suffer from two major drawbacks.

- The output of an encryption algorithm seems to be random, making any further compression impossible.
- The correlation of the plaintext can be used for efficient attacks: even if no messages of the plaintext are known, the encryption algorithm could be inverted by maximising the correlation of the estimated plaintext. Shannon (1949) showed that such attacks are not possible in the case of independent data, which can be approximated by data compression prior to encryption.

Many encryption algorithms, like DES, have the following property: changing a single bit of the ciphertext makes half of the bits of the plaintext change statistically, and vice versa. This property is used to provide the integrity service, and if the encryption algorithm does not fulfil it, then a hash function with a similar property is necessary. Because of this, channel coding must be performed after encryption. Otherwise, a small probability of error in the channel would result in a high probability of error in the decrypted message. This is because integrity mechanisms cannot distinguish random errors from intended attacks, and they assume an error-free channel.

This requirement is not true in some applications of cryptology for digital TV broadcasting (Macq and Quisquater, 1995), where some desired characteristics, such as transcodability and transparency, show the interest in developing new approaches, in which the source coding is developed in combination with channel coding and cryptographic coding.

5.- The security system must be an integrated solution which can provide security services for all types of multimedia services and applications

All kinds of data, voice and audio applications should use the same application interface to require security services. This means that we are trying to propose an integrated solution that could be used by all the information, independently of its nature or the specific higher layer protocols.

6.- The security system must permit compatibility with network interconnection and environments such as Scenario B

The security system should be flexible enough to coexist with traffic from other networks. If the security services have already been supplied at the end terminals in the other networks, our system should allow this secure traffic without providing repeated security services. Moreover, insecure traffic from applications such as LAN interconnection should have the possibility to require security services.

7.- End-to-end security mechanisms must be used

This solution is better than link mechanisms from the security point of view. Moreover, link measures would imply the encryption and decryption of the cells at every network switch, with the corresponding key-management overhead. The only advantage of link measures is that address information is encrypted, enhancing privacy.

3 PLACEMENT OF THE SECURITY SERVICES

In this section, we present the main options for placing information encryption (which is necessary in order to provide confidentiality and integrity for bulk information), key management and authentication within the ATM layered architecture.

3.1 Information encryption. Confidentiality and integrity

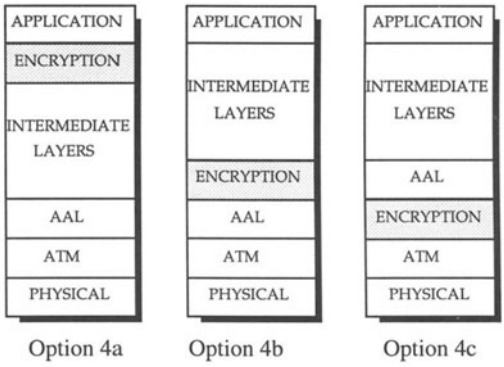

Figure 4 Three options to place the encryption.

The security services of confidentiality and integrity make use of the encryption mechanism. Therefore, the placement of these services would depend on the placement of the encryption mechanism. Encryption placement within the ATM Protocol Reference Model is complex and controversial. The three possibilities presented in Figure 4 must be considered.

The first possibility is to place it immediately below the application layer, as shown in Figure 4a. In this situation data from sensitive applications are ciphered at the source terminal before being passed to the lower layers, encapsulated with the corresponding communication protocols and sent through the network. At the destination point the reverse process is done and data are deciphered just below the application layer. This solution has several advantages: firstly, the amount of data to be enciphered is reduced, inasmuch as the headers of the layers below application are not processed (this facilitates requirement 3) ; secondly, the assignation of the suitable key is as easy as choosing a key for each application and then enciphering the sensitive data with this key (it highly facilitates requirements 1 and 2). Requirements 4 and 7 are also fulfilled, and this is the only solution that completely fulfils requirement 6 (this is the best for Scenario B). Nevertheless, this solution can hardly provide integration of all types of multimedia services (requirement 5). With this solution, a specific security layer should be built for all kinds of protocols below the application layer.

The lowest possible placement of encryption is between the ATM and AAL layers, as shown in Figure 4c, if we use end-to-end encryption (requirement 7). The header of the ATM cells must remain in cleartext to allow its routing from the source to the end point. In fact, link security is undesirable and today's technology does not permit encryption and decryption at each network switch. Requirement 5 is easily fulfilled, because all the information to be sent to the network must access this layer. Requirements 1 and 2 can be also fulfilled, though we need to devise primitives that access the ATM layer directly from the application layer to send the session key to its corresponding cipher, which is not an easy problem.

However, if this solution is adopted, we must expect that small information units (ATM cells) from different applications will reach the cipher and, therefore, the key must be changed. As a result, fast key switching is needed (in the worst case, each consecutive cell would belong to a different application, and due to the requirement 2 the cryptographic key must be changed every 48 bytes).or some ciphers must act in parallel, one for each application or channel, making requirement 3 more difficult to fulfil. In any case, the cost of the encryption device is much higher than in the above solutions. Furthermore, this solution is against requirement 4[1] because the AAL is responsible for handling transmission errors (i. e., the channel coding).

Placing the encryption immediately above the ATM Adaptation Layer (AAL), as shown in option 4b, makes requirements 1 and 2 much easier to achieve than option 4c. Moreover, the information blocks are greater, facilitating encryption efficiency and therefore requirement 3. The other requirements, except requirement 6, are easy to achieve. In fact this is the highest possible placement of encryption that fulfils requirement 5, because this is the top protocol defined for the B-ISDN, and all multimedia services and applications must access the AAL. Considerations about how this option can fulfil requirement 6 will be presented below.

To summarise, Table 1 shows the requirements fulfilled by each option. We can clearly see, for instance, that option 4b is better than option 4c for the stated requirements, and therefore

[1] In the CRIPTO project a self-synchronising stream cipher was necessary to handle channel errors, with some undesired characteristics, such as expansion of network errors. Otherwise, a single cell loss would break the connection.

option 4c has to be discarded. Option 4a also seems good, but the impossibility of fulfilling requirement 5 leads us to discard it, mainly because we are seeking an integrated solution. Consequently, option 4b is the most attractive, and following this option a security level should be layered on top of the AAL protocol that could provide privacy and reliability between broadband communicating applications, transparently for higher level protocols.

Table 1 Requirements fulfilled by each option

	OPTION 4a	*OPTION 4b*	*OPTION 4c*
REQUIREMENT 1	Very easy	Relatively easy	More difficult
REQUIREMENT 2	Very easy	Relatively easy	More difficult
REQUIREMENT 3	Yes	Yes	High requirements for the cipher
REQUIREMENT 4	Yes	Yes	NO
REQUIREMENT 5	NO	Yes	Yes
REQUIREMENT 6	Yes	Permits coexistence	Permits coexistence
REQUIREMENT 7	Yes	Yes	Yes

3.2 Key-management, authentication, access control and nonrepudiation

Only sensitive applications need to be secured. Consequently, key management should be placed at the application layer to obtain a suitable interface with applications and users. Authentication, like key management, should be placed at the application layer to provide a suitable interface with users and applications. Actually mutual authentication is necessary during the session-key negotiation. Later, the communication encrypted with this session-key will also be authenticated. Asymmetric cryptography has several advantages over symmetric cryptography when used for authentication. These include a more natural support for authentication to multiple recipients, better support for nonrepudiation (repudiation is a party's denial of having sent a message), and the elimination of secret encryption keys from the central server. Nonrepudiation is specific to some applications, and it makes use of asymmetric algorithms. It should therefore be placed at the application layer, like key-management, authentication and access control.

4 ARCHITECTURE OF THE SECURITY SYSTEM

With the above considerations, in Figure 5 we propose the security system's architecture. We only use the user plane of the B-ISDN Protocol Reference Model (see CCITT I.321, 1991). This means that we do not interfere with the network control and management for the sake of simplicity. We are aware that the use of the control and management plane would permit the integration of the security management in the network signalling, with several advantages (e. g., the security services could be negotiated as QoS parameters during the connection establishment period, and security services could be provided for the network management).

However, this would need a redefinition of network signalling and management, which is beyond the scope of this work.

The security protocol is composed of two layers: the Secure ATM Adaptation Layer (SEC-AAL) and the Secure Application Layer (SEC-APL).

At the lowest level, the SEC-AAL is layered on top of the ATM Adaptation Layer, and it is application protocol independent. A higher level protocol can layer on top of the SEC-SSL transparently. It provides the mechanisms for bulk encryption and the services of confidentiality and integrity.

The SEC-APL is placed at the application layer. The asymmetric encryption mechanism, as well as the key-management and the services of access control, nonrepudiation and authentication, are placed at this layer. The sensitive applications can require the security services they need through a suitable application interface (API), which must specify security primitives to be used by applications.

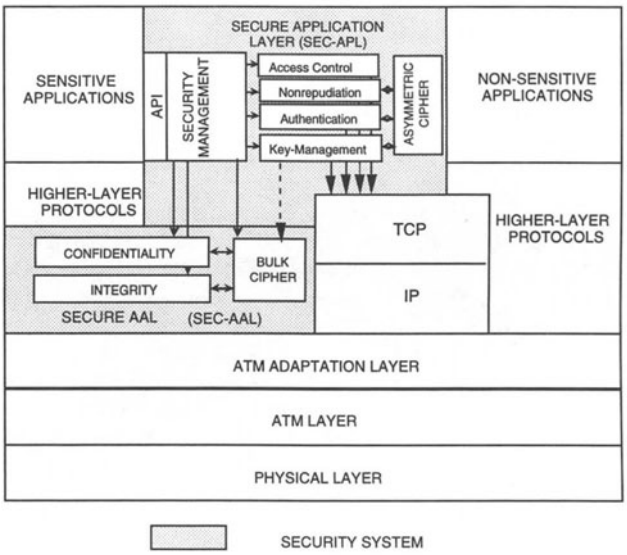

Figure 5 Architecture of the security system.

To illustrate how the security system works, let us to show an example. Suppose that a sensitive application on a local multimedia terminal (represented on the left side of Figure 5) requires a confidential connection with a remote application running on a remote terminal. The following steps, shown in Figure 6, must be carried out:

1.-The application (AP) demands the confidentiality service to the secure management module (SMM) through the Application Interface (API) by means of a well defined primitive function.

2.-The SMM wakes up the Key Management Module (KMM) in order to negotiate a Session Key (SK) to be sent to the bulk cipher.

3.-The KMM negotiates an SK with the remote entity according to an authenticated key-management protocol, which makes use of the Asymmetric Cipher (AC). This protocol uses a reliable communications protocol (e. g., TCP/IP). When this protocol is finished, both the local and the remote KMMs have agreed on a SK to be used for both Bulk Ciphers (BCs) to encrypt the connection.

4.-This SK and its Application Identifier (AI) are sent to the confidentiality module (CM) at the SEC-AAL and the SK is loaded in the BC.

5.-The AP is acknowledged that the CM of the SEC-AAL layer is ready to provide the required service.

6.- The AP begins the confidential connection by sending the information to the communication protocol stack. When this information reaches the SEC-AAL layer, its AI makes the CM send it to the bulk cipher to be encrypted with the suitable key (each AI has its associated SK).

7.-Then the encrypted information is sent to the network through the ATM Adaptation Layer.

At the remote terminal a similar process is done and the information is decrypted with the same SK. When the confidential connection is finished, the Secure Management Module is acknowledged by the Application and it resets the Bulk Cipher. For non-sensitive applications the security system is transparent.

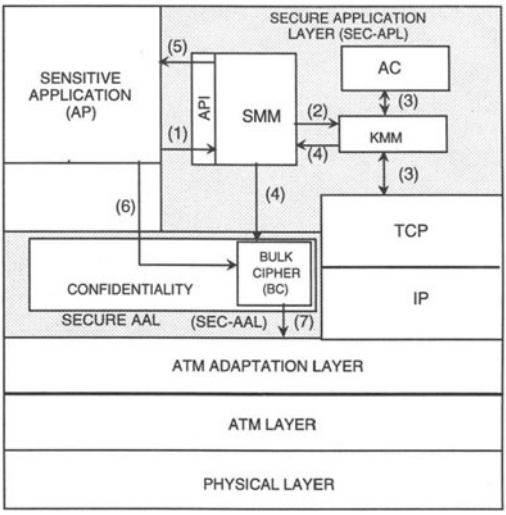

Figure 6 An example of the steps to establish a confidential connection.

5 COMPATIBILITY WITH SCENARIO B

In this section we study whether the proposed security system can fulfil requirement 6: "The security system must permit compatibility with network interconnection and environments such as Scenario B".

When two different systems can communicate with each other it is because they share a common protocol. In B-ISDN this protocol is specified by the B-ISDN Protocol Reference Model (CCITT I.321). Systems connected to other types of networks will share another protocol specification to communicate within their network. Interconnection of different networks is possible because systems can communicate through a shared family of protocols placed at higher layers. One example of these higher layer protocols is the TCP/IP family, which is used by Internet to build the widest computer interconnection scenario ever seen. In such a network each host is associated with an IP address, which is used to route the information through a virtual network, called Internet, without restrictions due to the physical network where the host is connected to. Without loss of generality, we can study the compatibility of the security system proposed in Section 4 with scenarios like Scenario B (Figure 2, Section 1), assuming that the end systems share the TCP/IP protocol suite (i. e., they are connected to Internet).

As an example, we come back to Figure 2 and we assume that MT1 and MT3 are connected to Internet (i. e., they both use TCP/IP) and, for instance, MT1 opens a connection (e. g., telnet) with MT3. To provide confidentiality or integrity, requirement 7 leads us to place bulk encryption at the top of the IP layer (the IP header cannot be encrypted to permit information routing). Mutual fulfilment of requirements 4 and 5 would place bulk encryption on top of a reliable protocol (e. g., TCP)[1]. Anyway, MT3 can never use the security system proposed in Section 4, because it is not directly connected to the B-ISDN and therefore cannot access the SEC-AAL layer. The information must therefore be encrypted at any level from the IP layer to the application layer, with a specific Internet security protocol.

The requirement of compatibility means that the proposed security system must permit other security protocols provided at higher layers. This is easily achieved because we provide security services depending on the application requirements. If applications are secured at any higher layer, then security services are not required to the secure management module of the SEC-APL layer, and the SEC-SSL layer considers this application as a non-sensitive application.

The other compatibility requirement is to allow secure interconnection of LANs and MANs through B-ISDN. This can be achieved if the SEC-APL and SEC-AAL are offered by the relays that interconnect the other networks with B-ISDN. Recacha et al. (1993) give an example of how relay devices can be used to provide security services to interconnect secure networks through an insecure network.

6 CONCLUSIONS

In this paper we have proposed an integrated solution for providing security services for all applications and services that will use the future Broadband Integrated Services Digital Network (B-ISDN). We have stated a set of requirements for the security system, and analysing these requirements we have proposed where the services of confidentiality and integrity should be placed within the B-ISDN Protocol Reference Model. We have also proposed the best placement of access control, nonrepudiation, authentication and key management.

---

[1] Actually there is a security protocol for the Internet, called SSL, which places bulk encryption at this layer.

We then propose a security system that can not only guarantee security services for all kinds of sensitive multimedia applications, but can also be transparent for applications that make use of other security protocols, allowing secure communication with terminals belonging to different LANs and MANs interconnected to B-ISDN.

7 REFERENCES

CCITT Recommendation I.121. (1991) Broadband Aspects of ISDN.

CCITT Recommendation I.321. (1991) B-ISDN Protocol Reference Model and its Applications.

Cruselles, E. et al. (1995) Secure Communications in Broadband Networks. *Proceedings of the 3rd. International Conference on Telecommunication Systems*. Nashville, TE. March 1995. pp. 114-122.

Guía de la, D. et al. (1994) ASIC_CRIPTO: un Circuito Integrado para el Módulo de Seguridad del PLANBA. *Proceedings III Reunión Española sobre Criptología*. Barcelona (Spain). December 1994. pp. 14-26. *(in Spanish)*.

Forné J., et al. (1995) The CRIPTO Project Architecture: A Spanish Experience in Broadband Networks Security. *Proceedings of the ICC'95*. Seattle, WA. June 1995.

Macq, B. M. and Quisquater, J. J. (1995) Cryptology for digital TV broadcasting, *Proc. of the IEEE*, vol. 83, no. 6, pp. 944-957.

Martínez del Cerro, F. J., Fernández-Amigo Barranco, J. (1993) "Servicios multimedia: TEMA/PLANBA". *Comunicaciones de Telefónica I+D*. Vol. 4, N° 2, *(in Spanish)*.

Recacha, F. et al. (1993) Secure Communications in Extended Ethernet Environments. *IEEE Journal on Selected Areas in Communications*. Volume 11. Number 5.

Rueppel, R. A.,(1986) *Analysis and Design of Stream Ciphers*. Springer-Verlag.

Shannon, C. E. (1949) Communication theory of secret systems, *Bell Syst. Tech J.*, vol. 28, no. 4, pp. 656-715.

8 BIOGRAPHY

Jordi Forné is a Lecturer at the Department of Applied Mathematics and Telematics of the Polytechnic University of Catalonia at Barcelona, Spain. His research interests include broadband communications, information and network security and cryptography.

José Luis Melús is an Associate Professor at the Department of Applied Mathematics and Telematics of the Polytechnic University of Catalonia. His research interests include modelling and simulation of multiprocessor systems, digital communications, packet communications, coding and cryptography. Currently he leads the research group on Cryptography and Data Security at the Polytechnic University of Catalonia.