ISDN SECURITY SERVICES

Merging ISDN and ATM security requirements

Herbert Leitold, Karl Christian Posch, Reinhard Posch
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria
Herbert.Leitold@iaik.at
Karl.Posch@iaik.at
Reinhard.Posch@iaik.at

Key words ISDN security, ISDN channel security, ISDN encryption

Abstract Analog and digital plain old telephony service (POTS) is increasingly replaced by technologies that integrate voice, data, and video communication services. The integrated services digital network (ISDN) offers the embedding of this advanced multimedia communication into the subscriber loop. Nowadays widely available, ISDN builds a promising approach to improve company's, public authority's, or individual's telecommunication facilities. However, a secure means of transferring sensitive information in any publicly accessible communication infrastructure is a major concern. In particular, authenticated and confidential communication is of paramount importance.

In this paper, we describe the implementation of a paradigm where advanced security services are offered by the ISDN infrastructure as an additional service. The encryption model is based on transparently integrating the security devices into the ISDN network termination (NT). This makes the approach independent from both the terminal equipment (TE), and the service used, as well as independent from the ISDN switches and exchanges installed by the service provider. The paper discusses integration of the security device into the ISDN architecture, as well as the design of a data encryption standard (DES) TripleDES encryption unit being the buttress of the ISDN security solution. Comparisons to related work and products in the field are made and the relation of the project to the broadband pendant to ISDN—broadband-ISDN (B-ISDN)—is sketched.

B. Preneel (ed.), *Secure Information Networks*

1. INTRODUCTION

For decades, residential telecommunication has been restricted to the public switched telephone network (PSTN). Communication requirements beyond voice services such as dial-in Internet access and computer-based data communication have been discontentedly met by using modems to get digital data over the hurdle of an analog bearer service. Advances in computing and communication merged the two fields, and integrated services digital network (ISDN) [1] has promised to fit both needs since the early 1990's [2] [3]. With transfer rates ranging from 128 kbps (basic access BA) up to 2 Mbps (primary rate interface PRI) ISDN has influenced telecommunication since its first pilot installations [4] [5]. One of the main advantages offered by ISDN is the integration of different services, such as voice communication, video telephony, facsimile document transfer, digital data communication, or X.25 packet-switched services [6].

However, the emerging integration of ISDN into company's and public authority's communication facilities urgently demands for a secure means of transferring sensitive information. A set of security requirements has been identified by [7], or by the ISDN Security Architecture of the North American ISDN User Group (NIUG), respectively [8]. The identified security requirements are data integrity, non-repudiation, data confidentiality, authentication, and access control. In this paper the primary scope is data confidentiality and end system authentication.

Recent work in the field of ISDN security resulted in a number of products offering data confidentiality and authentication. The approaches followed can be classified into two categories: On the one hand, security services can be integrated into the terminal equipment (TE), i.e. the end system device. An example for this approach is described in [9], a system where an encryption device is integrated into an ISDN internet protocol (IP) internet packet exchange (IPX) router. The second class of approaches is to install an intermediate device between the TE and the ISDN network terminator (NT). A representative of this class of products is found in [10]. As will be discussed later on, both approaches suffer from several disadvantages. The major disadvantage is that the solutions restrict confidentiality services to a limited set of TEs or services. Thus, the approaches counteract the service integration offered by ISDN.

In the project described in this paper an alternative route is taken. In co-operation with Telekom Austria as ISDN service provider, a secure ISDN NT (SecureNT) is being developed. The security device is based on an encryption unit that is integrated into the network termination in a way that

the interfaces to both the customer premises equipment (CPE), and the ISDN switch at the service provider side remain unchanged. The advantage is obvious: SecureNT is transparent to both the ISDN TE and the ISDN switch. Thus, neither the TE, nor the switch are to be modified when migrating ISDN to a secure infrastructure.

The basic block of SecureNT is a key-agile data encryption standard (DES) [11] encryption unit featuring electronic code book (ECB) and cipher block chaining (CBC) as operational modes [12]. The 112 bit effective key derivative TripleDES [13] is implemented to support strong cryptography. The term *key-agile* origins from [14], where confidentiality in asynchronous transfer mode (ATM) networks requires to switch rapidly between the session keys assigned to different user channels, so-called *virtual connections* (VCs) in ATM terminology. Although the bandwidth and timing constraints are different in ISDN, the requirement of switching between the session keys assigned to ISDN channels is similar.

The nexus to ATM is not drawn accidentally: ATM is the basic technology of the high-speed pendant to ISDN, known under broadband-ISDN (B-ISDN). As a consequence, the ISDN security project described in the paper takes this synergy into account by designing the encryption unit in a way applicable to both platforms. In addition, ISDN security is lacking a binding standard framework, except for the special application case of H.221 audiovisual teleservices, where a data privacy standard has recently been established [15]. By adapting security service procedures found in the ATM field, where there are ongoing standardisation efforts [16] [17], we stick to established procedures.

The remainder of the paper discusses the ISDN security solution. Section 2 gives an introduction to ISDN. The protocol reference model is discussed, and the alternatives to embed security devices into the reference architecture are addressed. Section 3 continues by addressing the security service negotiation schemes used to perform key exchange and end-system authentication. In section 4, the integration of the DES/TripleDES encryption unit into the ISDN NT is discussed. Alternatives are identified and the design of the encryption core is sketched. Finally, conclusions are drawn and the current state of the project is described.

2. ISDN BASICS

In this section the basics of ISDN are given. First, general aspects are described. This is followed by a description of the ISDN protocol structure at

the user network interface (UNI). Finally, the ISDN reference points and functional grouping are addressed, including a discussion of different ways to integrate security devices.

The characteristics of ISDN are basically described by a decomposition of its name: *Digital network* indicates the digital usage of the subscriber loop. *Integrated services* means that a variety of services, as divers as voice communication, videotelephony, or digital data communication are defined, including supplementary services, such as reverse charging, three party services, call forwarding, calling line identification presentation (CLIP), and so forth. Moreover, ISDN defines circuit switched communication, leased lines, as well as packet switched X.25 communication services.

Two different interfaces are defined at the UNI, the basic access (BA) and the primary rate interface (PRI). The BA has two B-channels, B_1 and B_2, with 64 kbps each. In addition, the D-channel with 16 kbps is defined. The PRI has 30 B-channels, B_1 to B_{30}, with 64 kbps each. The D-channel of the PRI has a transfer rate of 64 kbps. The distinction between B-channel and D-channel indicates a major characteristic of ISDN, the separation of signalling and user communication. This is described on the basis of the protocol model, as defined in the I.400 series specifications [18].

Figure 1 shows the ISDN protocol architecture and its relationship to the open systems interaction (OSI) reference model: The physical interface for BA and PRI corresponds to OSI layer 1, where B-channels and D-channels are multiplexed over the same physical interface. Above layer 1, the protocol structure for the two channels differ.

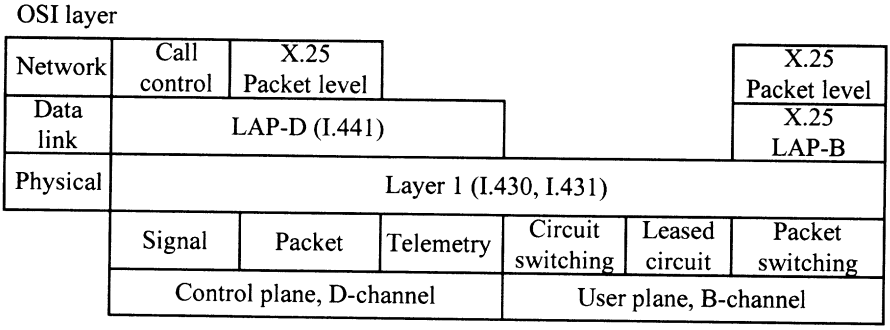

Figure 1. ISDN protocol architecture

For the D-channel, a new data link layer standard (link access procedure for the D-channel, LAPD) has been defined. This standard is based on

high-level data link control (HDLC), which is modified to meet ISDN requirements. The D-channel part in figure 1 supports an exchange of service primitives, which are used to establish, maintain, and terminate connections on B-channels. This is done invoking the digital subscriber signalling system no. 1 (DSS-1) call control protocol [19]. The D-channel can also support X.25 packet-switched data transmission, which is transmitted in LAPD frames. The X.25 level 3 protocol is used to establish virtual circuits on the D-channel and to exchange packet switched data.

The B-channel part in figure 1 enables voice, data, and image communication. For data communication, the B-channel can be used for circuit switching, semi-permanent or leased circuits, and X.25 packet switching. For circuit switching, a circuit is established on demand on the B-channel which provides a transparent data path between end-users. A semi-permanent or leased circuit is a B-channel circuit that is established by prior agreement between the connected end-users and the network. With either a circuit-switched connection or a semi-permanent circuit, the connected stations seem to have a direct, full-duplex link. They are free to use their own formats, protocols, and frame synchronisation. In the case of packet switching, a circuit-switched connection to a packet switched node is established on a B-channel using the D-channel control protocol.

Note, that the concept of separating the signalling channel—the control plane—and the user communication channels—the user plane—is continued in the ATM protocol reference model. Even the ATM signalling protocol elements (Q.2931) are derived from the ISDN signalling elements in DSS-1 (Q.931). This gives a close relationship between security requirements and concepts in both technologies ISDN and ATM.

Having described the protocol basics of ISDN, we continue with a description of the reference architecture and functional grouping of ISDN. This is done on the basis of the reference points, where security devices can be included into the reference model. Figure 2 illustrates the reference model. At the user side, end system components can be ISDN protocol compliant TE_1 type devices or conventional analog TE_2 type components, where a terminal adapter (TA) converts between the ISDN and non-ISDN protocols. Therefore, reference interface points R and S are defined. The ISDN network is terminated at reference point U, the twisted pair copper wire of the subscriber loop. At reference point T the network termination (NT) is divided into two functional groups, NT_1 performs line termination, layer 1 multiplexing, and power transfer. NT_2 performs layer 2 and layer 3 protocol handling and multiplexing. In many cases NT_1 and NT_2 are integrated into one unit, sketched as NT in figure 2.

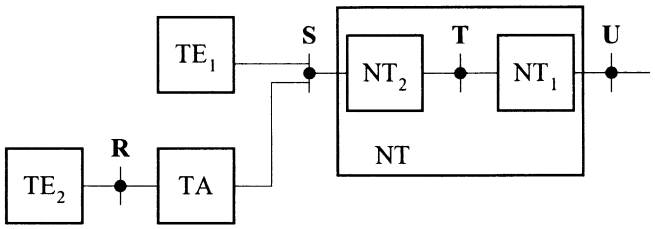

Figure 2. ISDN reference points and functional grouping

Security devices can be integrated into the TE components, with the obvious drawback of limiting the security services to this certain type of equipment. An alternative is to split at the reference point S and insert an intercepting unit. However, this has to take into consideration that different S-interface configurations are defined: At the BA, the S-reference point can be installed in a point-to-multipoint configuration, the so-called S_0 bus allowing to attach up to eight TEs to the reference point S. On the other hand, a point-to-point configuration of the BA or PRI is commonly used to connect to a private branch exchange (PBX). Such PBXs integrate NT_2 functions in many cases. This points out a drawback of the reference point S ISDN security approach. The concepts are focused on the S_0 bus, thus, PBXs at the S or T reference point cannot be integrated into the security domain.

As a consequence of the drawbacks identified, we follow the concept of integrating the security functions into the NT at the interface between the U-transceiver and the S/T-interface block. To achieve confidential communication, two general functions are required: First, security services negotiation to authenticate the communicating partners and to establish session keys is needed. The second functional block is the encryption process. The former—embedding security services negotiation into the ISDN model—is described in section 3.

3. SECURITY SERVICES NEGOTIATION

In this section we discuss how the negotiation of security parameters is embedded. A transparent communication channel is required between the end systems. Two alternatives are worth considering: embedding this channel into the control plane, or using the user plane:

- D-channel: As session keys are required prior to starting the user communication, the security service can be negotiated as part of the

signalling protocol used to establish the user plane channels. This is a method defined in [17] for ATM networks.

- B-channel: The alternative is to embed security services negotiation into the user plane.

Defining additional signalling information elements (IEs) to enhance the signalling protocol sounds promising. However, there are two drawbacks: On the one hand, the DSS-1 signalling channel is not a transparent end-to-end channel. The D-channel is terminated at the ingress ISDN switch and converted to the inter-switch protocol signalling system no. 7 (SS-7) [20]. Thus, the ISDN switches interpret the signalling IEs and would need to be upgraded to additional security IEs. The second drawback is that encrypting the B-channels requires explicit synchronisation points between the encrypting and decrypting end. Whereas the B-channels are synchronous 64 kpbs lines, real-time constraints are not given in the control plane.

Consequently, the alternative chosen is to perform security services negotiation via the B-channel. Following a concept termed user plane blocking [17], the security services and session key negotiation procedures are granted exclusive access to the B-channel immediately after the call is established. This is shown in figure 3 on the basis of the signalling messages for the TE initiating a call.

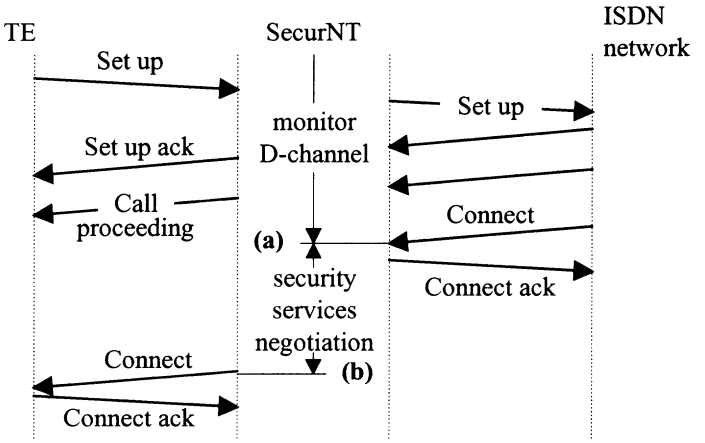

Figure 3. Security services negotiation phase

As illustrated in figure 3, SecureNT monitors the D-channel to identify the establishment of a call. The signalling protocol elements are transparently passed between the TE and the ISDN network, except the *Connect* message indicating that the B-channel is established. SecureNT

withholds this message and generates a *Connect ack*. Indicated as *(a)* in figure 3, this results in a situation where the B-channel is established between the two SecureNT devices, but not between the communicating TEs. Consequently, the B-channel can be used for session key negotiation and exchange of security parameters, such as certificates. Upon completion of the session key exchange procedures, SecureNT initiates an encryption synchronisation sequence and hands over the B-channel to the TE by forwarding the previously withheld *Connect* message. This is sketched as *(b)* in figure 3.

During the security services negotiation phase, X.509 certificates are exchanged to perform end system authentication. Diffie-Hellman key exchange [21] is used. In order to be capable of replacing the session key establishment procedures upon user requirements or legislative needs, a microprocessor is used for these purposes. With reference to figure 1, the microprocessor is employed to implement the D-channel control protocols to perform the user plane blocking.

4. ISDN ENCRYPTION USING AN ATM KEY AGILE UNIT

As has been described in previous sections, there are various options for including encryption into an ISDN channel. Even when concentrating on the set-up preferred in this paper, which is illustrated in figure 4, we still have a broad range of options for implementing symmetric encryption. For the sake of simplicity, although not a necessity, we narrow our scope to TripleDES witch electronic codebook mode (ECB) and cipher block chaining (CBC) mode only.

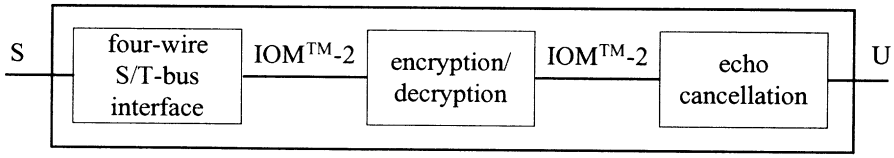

Figure 4. ISDN encryption inside a network termination unit

In this section, typical structural scenarios will be explored and the features of one particular solution will be explained in some detail. The motivation for preferring this particular solution has been the involvement of the system designers in two parallel projects, ISDN encryption and ATM

key agile encryption. Factoring out the common functional features of an encryption unit capable for serving both scenes showed that a two-mode encryption system could be obtained by only slightly augmenting the ATM key agile system.

Between the U-interface unit (e.g. an echo cancellation unit) and the four-wire S/T-bus interface inside an ISDN network terminator (NT) one typically can find two bit-serial channels, one for each communication direction, plus a clock signal for bit synchronisation and a frame-synchronising signal. The solution described here intercepts at this point by extracting octets from and inserting octets into this channel.

Figure 5 illustrates this interception unit together with several encryption units. The beginning of a frame lasting for 125 μs is indicated by the frame synchronising clock (FSC) signal. During a frame, 4 octets carrying information for channel B_1 and B_2, a monitor channel, and finally channel D are transmitted in each direction. These 32 bits are synchronised with the data clock (DCL) signal.

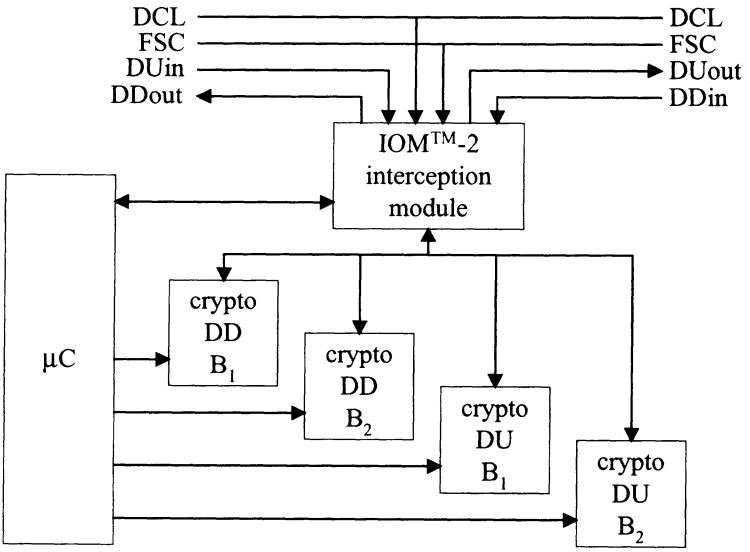

Figure 5. Basic ISDN encryption set-up

In principle, we need four symmetric encryption units for the two channels, B_1 and B_2, in both directions, upstream and downstream. In addition, a micro-controller is used for setting up confidential keys between the two NTs. This micro-controller provides all software flexibility needed

in the system for setting up the confidential communication channels, whereas the four symmetric encryption units are in charge of real-time encryption.

An alternative approach is illustrated in figure 6. This solution only employs one encryption unit serving all four communication channels multiplexed in time. Here, buffers are necessary for collecting octets until an encryption block of, say, 8 octets is available. Still, the micro-controller needs to take care of setting up the keys, is in charge of handling the D-channel communication, and needs to provide in real-time two to four keys for the multiplexed encryption unit.

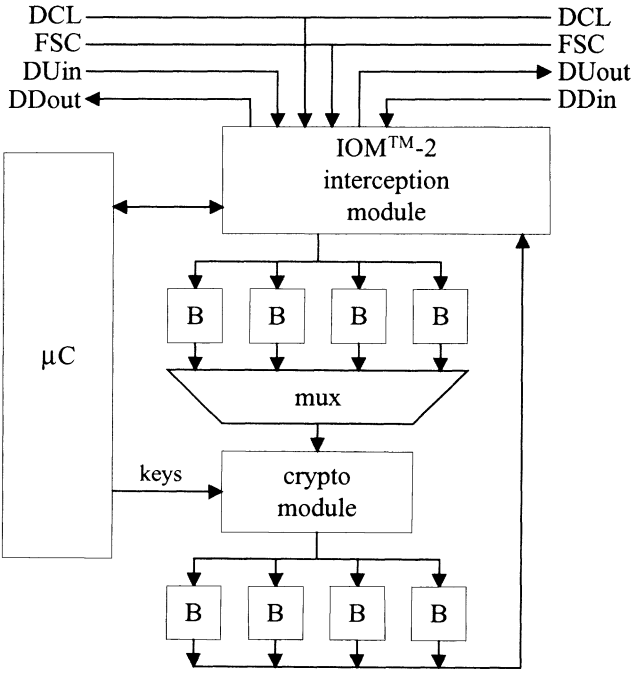

Figure 6. Time-multiplexed encryption unit

The benefit of this system is that only one encryption unit needs to be employed. ISDN channels are slow enough that today's TripleDES encryption hardware is easily capable of handling all four ISDN channels found in a network terminator. And the job of buffering adds up to 64 octets only. But, handling keys in real-time and in addition to take care of the D-channel keeps the micro-controller rather busy.

Therefore, a solution is preferable which also would handle real-time key management inside the encryption unit. When speaking about keys, we also include the initialisation vectors (IV) for cipher block chaining mode encryption. As an example let us have a look at a DES unit: Time-multiplexing in a TripleDES unit doing two-key TripleDES encryption in CBC mode involves providing 128 bits of keys, unloading the previous 64 bits for later use as an IV, and loading 64 bits of IV for the new block. With a 16-bit micro-controller this would ask for handling one word per 2 μs.

In principle, the same problem is faced in ATM encryption. When using key agile encryption for ATM, the encryption unit has its own store for keys and IVs. This memory typically consists of a content-addressable memory (CAM) which allows fast searching of key indices indicated in the virtual path, virtual channel identifier (VPI/VCI) field of the header of some ATM cell. With this key the following payload of the ATM cell is to be encrypted or decrypted. Typically, two consecutive ATM cells have a different VPI/VCI, so unloading data for later use as an IV, and loading of new keys and the IV is involved at the beginning of each ATM cell.

So, why not use an ATM key agile encryption system for ISDN. Then, the micro-controller would provide faked ATM headers to fool the ATM encryption unit. These pseudo-headers include pointers to keys stored in the CAM. Loading the CAM with keys is easy through sending ATM management cells carrying the keys. Such cells are recognised by the ATM key agile encryption unit, and appropriate action is performed inside this unit. Producing such cells does not put any hard real-time constraint onto the micro-controller.

In the context of the project Secure Communication in ATM Networks (SCAN) funded by the European Commission under the Advanced Communications Technologies and Services (ACTS) Programme, the authors of this paper have been involved in designing a microchip for an ATM key agile system [22]. Enhancing this system with additional hardware functions such that it can be also used in the ISDN arena is rather straight forward and almost negligible in terms of silicon area. Figure 7 illustrates such a system.

Apparently, only a tiny CAM is needed in the case of ISDN—only a few key sets need to be loaded into the ATM crypto module—whereas in the case of ATM encryption we face dozens and hundreds of keys. Therefore, the CAM is split into a small on-chip section and an external CAM. If this microchip is used for ISDN encryption, usually no off-chip CAM is needed.

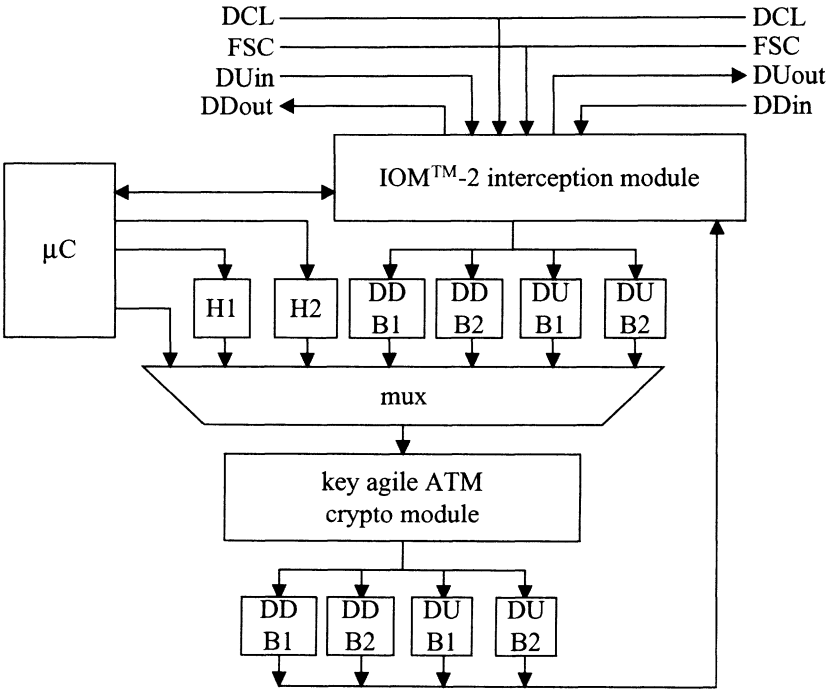

Figure 7. ISDN encryption involving a key agile ATM crypto module

In the following we will describe the ATM key agile encryption unit in more detail, and show how its dual-mode interface is used for ISDN encryption. A block diagram of this unit is shown in figure 8. Basically, the ATM encryption unit is inserted at the UTOPIA interface between the ATM layer and the physical layer. This interface is accessible and defined on all relevant ATM network cards. UTOPIA is a clocked octet-wide interface with two line hand-shaking at 25 MHz clock rate. In addition, there is an extra "start-of-cell"-bit for synchronisation on cell level. The ATM encryption unit has four such uni-directional interfaces, two per communication direction. The chip recognises special ATM cells carrying information for configuring the ATM encryption unit. Basically, these cells are used for loading new keys into the CAM, or for invalidating keys in the CAM. Such cells have a special VPI/VCI which is loaded into the chip during its initialisation phase using VPI/VCI equal 0. Once a key is stored in the CAM, it can be referred to by using its associated VPI/VCI. The ATM encryption unit recognises ATM header blocks with their VPI/VCI, and tries to locate the keys in the CAM. In case of finding the keys in the CAM, it

subsequently unloads and stores the current block in the CAM for potential later usage as IV, and loads the new keys and the IV into the encryption core. In case of a miss in the CAM, the handling of the cell depends on the payload type identifier (PTI) contained in the ATM cell header. It is either transmitted without alteration, or not communicated to the UTOPIA output at all. The ATM encryption unit can handle 155 Mbps in both directions simultaneously. The bottle-neck of the overall operation lies in the speed of exchanging keys and IV between CAM and encryption core.

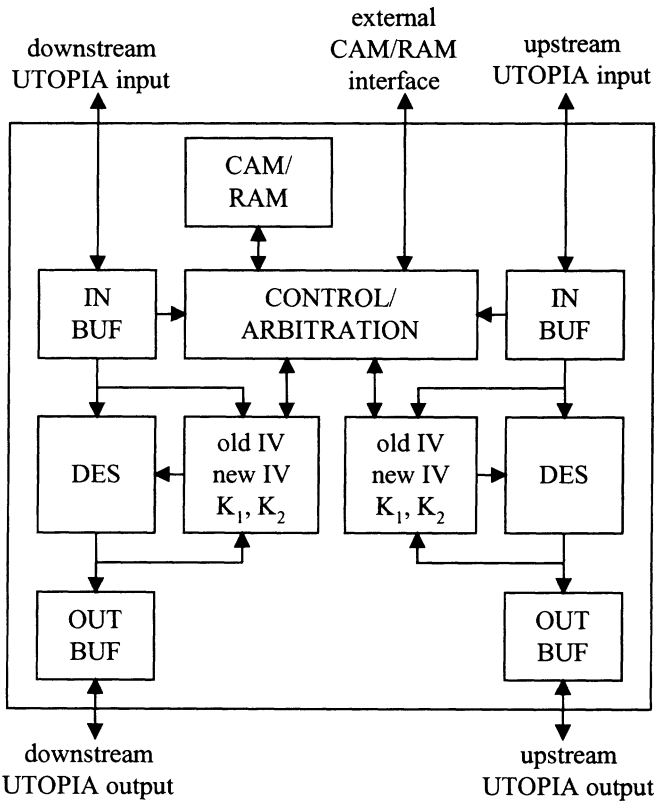

Figure 8. Block diagram of key agile ATM encryption module

When using this chip for ISDN encryption, most I/O pins are not needed with their ATM functionality. There is no need for the 24 UTOPIA interface pins, nor do we need the pins for accessing the external CAM. Therefore, these pins may be used alternatively for connecting to the micro-controller with a data width of either 8 or 16 bits. The various I/O registers as seen by

the micro-controller are mapped to addresses, i.e. the ISDN/ATM encryption unit acts like an intelligent I/O device in this mode. Loading keys from the micro-controller to the CAM is achieved by writing the sequence of octets of the key-download cell to a particular output register. Two buffers, H1 and H2 in figure 7, hold 5-byte headers containing pseudo-VPI/VCIs. Each of these two buffers is mapped to an output register, and a sequence of 5 write cycles issued by the micro-controller alters the information in any of those buffers. Whenever 8 octets have been collected by the interception unit, an train of 5 plus 8 octets is issued toward the key agile encryption unit. As there are 4 potential sources for this, a simple round robin arbitration is needed. Adding a substantial amount of header information to each block of 8 octets is of no relevance, as ATM speed is far beyond ISDN speed. The size of the input buffers is set such that real-time operation is possible even in the worst case.

The interception unit mainly consists of shift-registers for serial/parallel and parallel/serial conversion, plus some additional registers and a counter/decoder unit synchronised by the FSC signal in order to keep track of the individual bits coming in and going out serially.

5. CONCLUSIONS

The paper has described a project aiming to provide confidential communication in ISDN networks. For concerns of service independence, as well as independence from the end system, the approach of integrating the security devices into the ISDN network termination has been followed. Therefore, the ISDN data stream is accessed at a well-defined interface in the ISDN NT.

The architecture of the DES, TripleDES encryption unit as the core piece has been described in more detail. In particular, the synergies between ISDN and ATM security have been addressed. By describing different approaches to achieve the goal of confidential communication in ISDN, the reasoning of using an ATM key agile encryption unit has been given.

Currently, the overall system is being designed and first engineering prototypes on silicon are expected to be available by end of 1999. The encryption unit has an on-chip oscillator with a variable frequency. In case of ATM encryption, the internal clock rate is set to 240 MHz. Some parts of the chip run at this high speed and are designed in full-custom design style. Other parts which do not need this speed use a slower clock rate gained by division. These are designed in semi-custom design style.

References

[1] G.C. Kessler, ISDN, Second Edition, MacGraw-Hill, 1993.

[2] P. Kahl, ISDN Implementation Strategies of the Deutsche Bundespost Telekom, IEEE Communications Magazine, v. 28, n. 4, 1990.

[3] J.P. Temime, Numeris-ISDN in France, IEEE Communications Magazine, v. 30, n. 8, 1992.

[4] R. Roy, ISDN applications at Tenneco Gas, IEEE Communications Magazine, v. 28, n. 4, 1990.

[5] C.S. Thachenkary, Integrated services digital network (ISDN): six case study assessments of a commercial application, Computer Networks and ISDN Systems, North Holland, v. 25, n. 8, 1993.

[6] J.D. Hunter, W.W. Ellington, ISDN: A Consumer Perspective, IEEE Communications Magazine, v. 30, n. 8, 1992.

[7] W. Burr, Security in ISDN, NIST special publication 500-189, 1991.

[8] ISEG, ISDN Security Architecture, ISDN Security Expert Group ISEG, North American ISDN User Group, NIUF 412-92, 1992.

[9] SecurPac™, IEM ISDN Encryption Module, Technical Specifications, Secure Network Solutions Ltd, 1999.

[10] Biodata, Handbuch Babylon S0, Biodata GmbH., 1999.

[11] ANSI, American National Standard for Data Encryption Algorithm (DEA), ANSI 3.92, American National Standards Institute, 1981.

[12] ANSI, American National Standard for Information Systems-Data Encryption Algorithm-Modes of Operation, ANSI 3.106, American National Standards Inst., 1983.

[13] W. Tuchman, Hellman Presents no Shortcut Solutions to DES, IEEE Spectrum, v. 17, n. 7, 1979.

[14] D. Stevenson, N. Hillery, G. Byrd, Secure Communications in ATM Networks, Communications of the ACM, v. 38, n. 3, 1995.

[15] ETSI, Telecommunication Security: Integrated Services Digital Network(ISDN); Confidentiality system for audiovisual services, European Telecommunication Standard ETS 300 840, 1998.

[16] M. Peyravian, T. Tarman, Asynchronous Transfer Mode Security, IEEE Networks, v. 11, n. 3, 1997.

[17] ATM Forum, ATM Security Specification, Version 1.0, ATM Forum Technical Committee, ATM-SEC-01.010, 1999.

[18] ITU-T, User network interface aspects, I.400 series, I.410 – I.450 International Telecommunication Union, Telecommunication Standardisation Sector, 1984.

[19] ITU-T, Digital Subscriber Signalling System No. 1 - Network Layer, Recommendations Q.930 – Q.940, International Telecommunication Union, Telecommunication Standardisation Sector, 1993.

[20] ITU-T, Signalling System No. 7, Recommendations Q.700 – Q.766, International Telecommunication Union, Telecommunication Standardisation Sector, 1988.

[21] W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on information theory, vol. 22, 1976.

[22] H. Leitold, U. Payer, R. Posch, A Hardware Independent Encryption Model for ATM Devices, Proceedings of 14th Annual Computer Security Applications Conference (ACSAC), Phoenix, 1998.