ATM NETWORK SECURITY

Requirements, Approaches, Standards, and the SCAN Solution

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

Key words: ATM security, ATM confidentiality, Key agile encryption

Abstract: Broadband networks based on the asynchronous transfer mode (ATM) are emerging rapidly. Both the technological component in terms of ATM infrastructure, as well as the area of applications requiring Quality of Services (QoS) by the means of bandwidth or delay constraints are covered by a variety of projects and products. However, given the increasing interest in applications such as governmental communication, transmission of medical information, or commercial applications, the necessity of providing secure means of delivering sensitive contents is apparent.

In this paper, we focus on security services in ATM networks. The variety of different approaches and solutions are categorised by the means of its common and distinct functionality, as well as certain advantages and disadvantages are discussed. In addition, the standardisation efforts by the leading group in that area—the ATM Forum—are outlined. Finally, the essentials of the project SCAN[3] are given, resulting in a comprehensive solution to security services in ATM networks.

[3] The project Secure Communication in ATM Networks (SCAN) is funded by the European Commission, Directorate General XIII under the Advanced Communications Technologies and Services (ACTS) Programme, project number AC330.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35581-8_35

T. Yongchareon et al. (eds.), *Intelligence in Networks*

1. INTRODUCTION

Broadband networking has evolved dramatically in the past few years. Especially the asynchronous transfer mode (ATM) has attracted attention in the area of high-speed communication, promising the integration of almost all communication profiles such as voice, video and computer-based multimedia communication. Having had its first broad deployment in the high-speed local area network (LAN) arena [1], the emerging deployment of ATM in the public wide area network (WAN) sector is going on, such as the Trans-European Network 34 Mbps (TEN-34) [2] and its 155 Mbps successor TEN-155. ATM builds the basis of broadband integrated services digital network (B-ISDN) and is to be considered as one of the key technologies of the data-highway initiatives aimed by the majority of industrial countries, as described by the User Requirements and Strategies for Application (URSA) report [3]. Beside the capability of carrying the variety of communication profiles, the importance of ATM in the broadband networking arena is emphasised by the fact that it is defined basically independent from the physical media. Consequently, as surveyed in [4] and [5], promising residential access methods, such as asymmetric digital subscriber line (ADSL), or fibre-coax hybrid cable television (CATV) networks are focused towards ATM, as expressed by Maxwell for ADSL [6], respectively by Hernandez-Valencia for cable-networks [7].

However, as soon as publicly accessible infrastructure is involved, security is a major concern. ATM distinguishes from other networking technologies by the means, that the need of investigating security services was recognised early, in fact prior to a broad deployment of ATM networks. Both the research community, and standardisation bodies have been the driving factors: On the one hand, a number of approaches to security in ATM networks have been published by scientists. On the other hand, the leading groups working on ATM standardisation—the ATM Forum—established a security working group in 1996 [8], resulting in the ATM Forum Security Framework [9], as well as the ATM Forum Security Specification 1.0 [10] which has been approved recently in February 1999.

In this paper, we discuss these different approaches. Therefore, the remainder of this paper is structured, as follows: Section 2 describes the basic security requirements given in ATM networks. This is followed by the discussion of different approaches to ATM security in section 3. The ATM Forum Security Specification 1.0 is described in section 4. Section 5 outlines the project Secure Communication in ATM Networks (SCAN) that implements above stated specification by the means of a secure ATM network interface card (ATM-NIC) and, finally, conclusions are drawn.

2. ATM SECURITY REQUIREMENTS

ATM is a cell relay technique operating on protocol data units (PDUs) of a fixed size, called ATM cells. Similar to other packet oriented networks, such as X.25 or Frame Relay, ATM is a connection oriented technology by the means of virtual channels (VCs). Using signalling procedures VCs are established on demand as switched virtual connections (SVCs), or as permanent virtual connections (PVCs).

Closely related to the integrated services digital network (ISDN) protocol reference model, the ATM respectively the B-ISDN protocol architecture has been standardised by the International Telecommunication Union, Telecommunication Standardisation Sector (ITU-T) in recommendation I.321 [11]. It consists of several planes: Firstly, the management plane to maintain the network operational. Secondly, the control plane defines the signalling functions needed to establish and control the communication channels (VCs). Finally, the user plane provides transfer of user data across ATM virtual channel connections (VCCs) or virtual path connections (VPCs). The ATM protocol reference model is illustrated in figure 1.

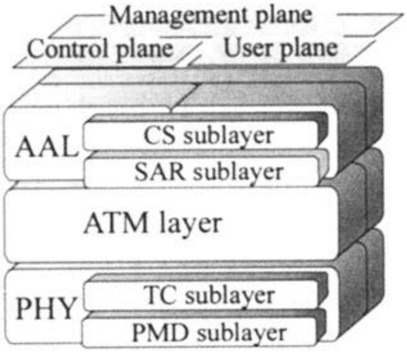

Figure 1. ATM (B-ISDN) protocol reference model

In addition to the planes, the ATM protocol reference model consists of several layers: At the top of the hierarchy the ATM adaptation layer (AAL) converts native ATM data or non-ATM information to the ATM cell format. Therefore, convergence sublayer (CS) and segmentation and reassembly (SAR) functions are employed. The ATM layer operates on ATM cells which consist of a five octet header used for guiding the information through the ATM network and a 48 octet payload that carries the user information. Finally, the physical layer embeds the ATM cell to the transmission frame, such as a synchronous digital hierarchy (SDH) frame. Therefore, transmission convergence (TC) and physical media dependant (PMD) functions are employed.

An ATM network consists of a set of ATM switches interconnected by point-to-point physical links. Two different types of interfaces are provided: Firstly, the user network interface (UNI) [12] between an user and an ATM switch, respectively between two ATM switches in some cases. Secondly, the network-network interface (NNI) [13] is defining the routing and signalling mechanisms needed within larger clouds of ATM switches. In addition, the UNI is subdivided into public-UNI and private-UNI, depending on whether the ATM link is connected to a public or private ATM switch.

From the security point of view an ATM network can be looked upon as a set of endpoints (users) interconnected by a set of ATM switches. Thus, the security interactions can be characterised as an user-to-user, an user-to-network, or a network-to-network interaction scenario. This is schematically depicted in figure 2. Two VCs are shown, VC_1 between end system A and end system C, and VC_2 between end system B and C.

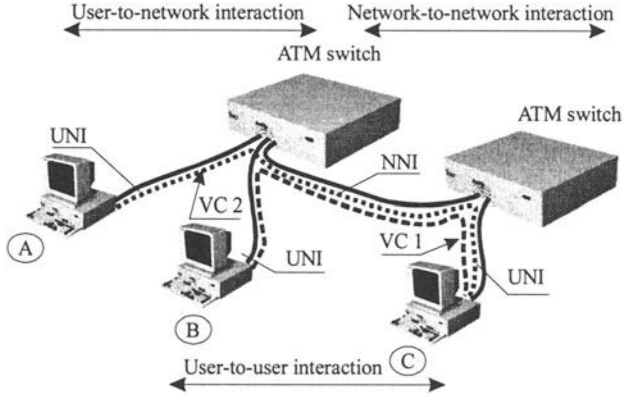

Figure 2. ATM security interaction model

With reference to the protocol model shown in figure 1, in particular the tasks assigned to the three planes, the security requirements are to be identified as follows:

- User plane: In the user plane providing transfer of user data across ATM VCCs or VPCs, four security requirements can be identified: Authentication, data confidentiality, data integrity, and access control. With reference to figure 2, these security requirements refer to the user-to-user interaction model.
- Control plane: The control plane performs connection establishment and connection maintenance functions. Both the user-to-network interaction model and the network-to-network scenario—as shown in figure 2—are

of importance. Since signalling message fraud affects the state and the availability of the network, the protection of control plane messages is of vital importance. Consequently, authentication and integrity are the basic security requirements.

- Management plane: The management plane performs management and coordination functions related to both the user, and the control plane. So far, ATM management plane security has not been that investigated in the literature. However, at least authentication and access control can be identified as security requirements.

It is worth mentioning that all approaches appearing in the literature have above listed requirements in common (see also [9]). Apart from the security features related to the different planes, a common functionality are the so-called support services, assisting the security services by providing key exchange, key update mechanisms, public key infrastructures, and further security parameter negotiation.

Having identified the basic security requirements, the following section 3 surveys the different approaches to security in ATM networks. Guided by a qualitative discussion of the advantages and the disadvantages of a certain class of approaches, the common features are discussed.

3. ATM SECURITY APPROACHES

In order to categorise the multitude of proposed and established approaches to ATM security, this section assigns the approaches to the protocol layer the cryptographic mechanisms are applied to: Subsection 3.1 discusses application layer security services, subsection 3.2 addresses AAL based approaches, subsection 3.3 investigates embedding of security services into the ATM layer, and PHY layer based approaches are discussed in subsection 3.4. Finally, support services are addressed in a separate subsection 3.5, as these services are rather related to the planes of the ATM protocol reference model, than to a certain layer.

3.1 Application layer security services

The first approach appearing in the literature is applying security services to the protocol layers located above the ATM protocol model. Such an approach, for instance integrating the security services into the network layer of the open system interconnect (OSI) model (e.g. Internet protocol IP), the OSI transport layer (e.g. Berkeley Software Distribution BSD sockets), or even the application itself (e.g., a secure hypertext transport protocol HTTPS server), makes the approach independent from ATM and, apart from the high transmissions rates in the multi-Mbps range offered by ATM, gives no substantial difference to well understood methods, such as IPSEC or secure socket layer (SSL).

However, this class of approaches is addressed in this paper to identify the major drawback: Due to the high bandwidth required, integrating cryptographic algorithms into applications fails for performance reasons. Hardware support is needed, hard to achieve at the protocol layers involved in a platform and service independent manner, as these protocols are usually implemented in software.

As one representative of this class of approaches, [14] is referenced: The work described by Ellermann and Benecke addresses the performance when introducing conventional firewalls into high-speed ATM networks.

3.2 AAL security services

The first class of approaches integrating security services into the ATM protocol model is applying them to the AAL. Especially for computer based traffic, this approach is alleged advantageous, as one certain AAL (AAL-5) is mainly used. The following figure 3 illustrates the two interfaces where security services can be integrated into the AAL. These are the interface between the two AAL sublayers CS and SAR which is shown as (a) in figure 3, respectively the interface between the AAL and the host computer's protocol stack which is shown as (b) in figure 3.

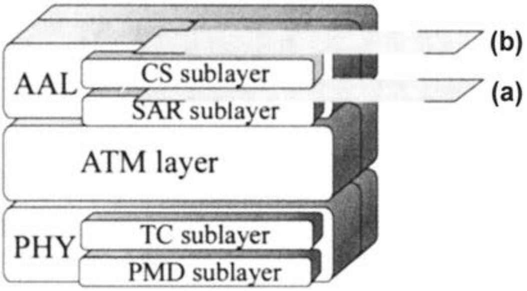

Figure 3. AAL security services embedding

AAL embedding of security services has been proposed several times. The main representatives of this approach are, as follows:

- General AAL approaches: For user plane confidentiality, Cruickshank, et. al proposed to encrypt the AAL-SDU payload [15]. A similar attempt to integrate security sevices into the AAL is described by Forné and Melús [16].

- CS-SAR interception: In the approach discussed by Geng, et. al. [17], the security services intercept the interface between the CS sublayer and the SAR sublayer of the AAL by introducing a data protection layer (DPL). In this approach, user plane confidentiality and user plane integrity are provided.
- Host-AAL interception: An alternative has been proposed by Chuang in [18], where a CryptoNode intercepts AAL frames at the direct memory access (DMA) interface between the host computer and the ATM-NIC. Targeting encryption of the user data, user plane confidentiality is provided in that approach. Comparable to this is a Solution for Frequent Communication (SFFC) given by Laurent, et. al. in [19], where the user plane confidentiality service is also layered above the AAL.

Above stated approaches have in common that the aim is to secure computer based communication in ATM network infrastructures. However, considering its implementation, two major drawbacks can be identified: On the one hand, the service independence ATM offers is counteracted, as the approaches are limited to that certain service class (AAL). On the other hand, at the high data rates to be supported the cryptographic algorithms are not feasible in a software implementation and state-of-the-art components to not offer the required hardware interfaces, except the DMA interface in the host-AAL interception approach described. In particular, user plane confidentiality using strong encryption algorithms requires hardware implementation of the cryptographic units.

Thus, it is to be concluded that, for user plane confidentiality, placing the security services in the AAL limits the flexibility in terms of service independence and faces implementation problems. However, for providing data integrity, integration into the AAL is advantageous, as the performance required for the message authentication codes (MAC) is feasible in software. In addition, the MAC can be transparently added to the AAL-SDU, whereas this is problematic in the ATM layer due to the fixed size of ATM cells.

Do cover that conflicting advantages and drawbacks, Cherukuri, Peyravian, and Wu conclude to integrate data integrity into the AAL, whereas data confidentiality is best located in the ATM layer [20]. This ATM layer approach is described in the following subsection 3.3.

3.3 ATM layer security services

Given the drawbacks regarding implementation concerns as described in the previous subsection, embedding data confidentiality into the ATM layer is advantageous. This makes the solution independent from the AAL and, thus, independent from the service class. In this approach, the 48 octet ATM cell payload is encrypted, by the way neatly fitting the block size of many symmetric block ciphers, such as the eight octet block size of the data encryption standard (DES) [21]. The five octet ATM cell header carrying the information to route ATM cells through the network is kept unchanged. Regarding embedding the cryptographic functions into the ATM protocol model, two opportunities exist:

- AAL-ATM interception: In [20], intercepting ATM cells at the interface between the AAL and the ATM layer is proposed. This is sketched as (a) in figure 4.
- ATM-PHY interception: As state-of-the-art very large scaled integrated circuits (VLSI) used for ATM end devices integrate both the ATM layer, and the AAL, access to the AAL-ATM interface is not given in many cases. An alternative is proposed in [22], where the interface between the ATM layer and the PHY layer is intercepted, sketched as (b) in figure 4. This interface is standardised as the universal test and operations physical interface for ATM (UTOPIA). UTOPIA is supported by almost any ATM component manufacturer. The approach is referred to as UTOPIA-intercepting encryption.

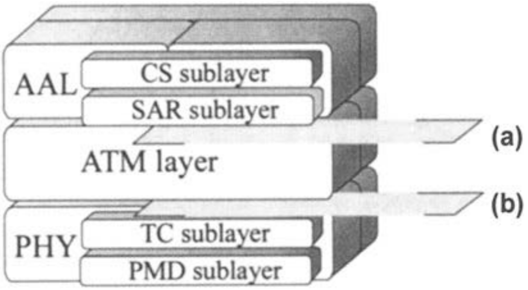

Figure 4. ATM cell level security services

Compared to AAL embedding, ATM layer embedding of security services has its main advantages for concerns of service independence when applying encryption, as stated above. However, beside the high data rates to be dealt with, in fact the same as in the AAL approach, an additional challenge is introduced: Due to the small cell payload, together with the fact that ATM cells assigned to different VCs arrive statistically multiplexed, the session keys used for encryption are to be changed rapidly, if unique keys are used for each VC. This has been termed key agile encryption by Stevenson, et. al. [23]. A further discussion of the key agility problem employing content addressable memory (CAM) techniques is given in [22].

3.4 PHY layer security services

Security services can be embedded into the PHY layer. This has been proposed by Rieke in [24]. In that approach providing data confidentiality, the whole ATM cell including the header information is encrypted. However, as the header information is to be interpreted by the intermediate ATM switches, as well as the virtual path identifier (VPI) virtual channel identifier (VCI) information is translated whilst passing an ATM switch, this approach requires decryption and re-encryption at each intermediate node. The user perceptive of endpoint-to-endpoint confidentiality in the user-to-user interaction scenario (see figure 2) inhibits this approach.

3.5 Support services

We complete this section by discussing how support services to perform key exchange or authentication protocols can be embedded into the ATM protocol model.

To perform authentication or to negotiate session keys, a transparent information channel is required. Three approaches exist, one related to the control plane, one to the user plane, and one employing management cells:

- Control plane information elements: Upon establishment of a VC, information elements (IE) carry the signalling data. The first approach to provide a support services communication channel is to enhance the signalling IEs by specific security IEs. This has the advantage of embedding the support services into the call setup phase and, thus, keys can be negotiated prior to the completion of VC establishment.
- User plane blocking: The disadvantage of additional signalling IEs is, that the ATM switches have to accept and transparently forward this additional information. An upgrade of the ATM network is required. In addition, the UNI version 3.1 does not provide sufficient information flows to perform three-way session key negotiation. A workaround is, to exclusively assign the VC to the support services for the period required for session key negotiation immediately after a VC has been established. Thus, the user plane is blocked for the application in that period.
- OAM flows: To re-negotiate session keys during a call, in-band operation and management (OAM) cells can carry the data. This is done using F4 flows on the VPC level, the VCC level uses F5 flows.

This completes the discussion of approaches to ATM network security. The approaches mainly address user plane confidentiality, data integrity, and authentication. In the following section 4 we continue in describing the ATM Forum Security Specification as a standards framework.

4. ATM FORUM SECURITY SPECIFICATION

The ATM Forum Security Specification 1.0 [10] has been approved in February 1999. With reference to the basic security requirements identified in section 2, the essentials of the ATM Forum approach are to be summarised, as follows:

- Entity authentication: Entity authentication is defined for the user plane. Either symmetric algorithms or asymmetric algorithms can be used.
- Data origin authentication and integrity: This is defined for the user plane and the control plane: In the user plane, MACs such as DES cipher block chaining (DES/CBC-MAC) are appended to the AAL-3/4 or the AAL-5 SDU. In the control plane this is accomplished between adjacent signalling elements by applying the user plane approach to the signalling channel.
- Data confidentiality: For confidentiality in the user plane, the ATM Forum follows the ATM layer approach, as described in section 3.3. Symmetrical encryption algorithms are defined, namely DES, TripleDES and FEAL in cipher block chaining (CBC), electronic code book (ECB), and a counter operational mode [25].
- Access control: User plane access control is defined on a per-VC basis using security labels. Access control is performed during connection establishment based on the security message exchange
- Support services: All three methods described in section 3.5 are defined, namely security IEs, user plane blocking, and using OAM flows. In addition, the security message exchange mechanisms provide for the exchange of X.509 public key certificates.

The ATM Forum Security Specification 1.0 constitutes a standards framework that enables interoperable solutions to secure communication in ATM networks. In the following section 5, we present a solution which results from a project the authors of this paper have been involved in.

5. THE SCAN PROJECT RESULT AND FINDINGS

The survey presented origins in the project SCAN, a project embedded into the European Commission Advanced Communications and Services (ACTS) Programme. The SCAN project objective is to provide confidential communication in ATM networks in an approach independent from the application, as well as the physical media ATM is applied to.

Streamlined to the ATM Forum Security Specification 1.0 [10], the project SCAN follows the UTOPIA interception approach described in section 3.3. An VLSI DES/TripleDES encryption unit intercepts the UTOPIA interface between the TC controller and the SAR processor of an ATM NIC. Note, that the term "*SAR processor*" refers to the VLSI integration of the ATM layer and the AAL common in state-of-the-art ATM end system components, as stated in section 3.2. The described scenario is illustrated in figure 5.

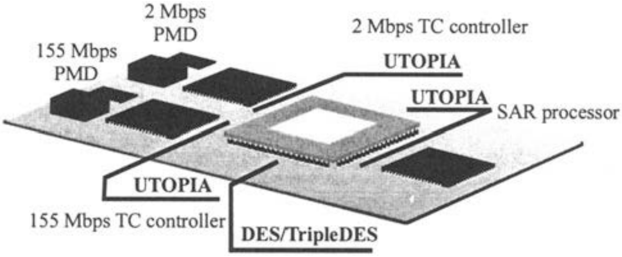

Figure 5. UTOPIA intercepting ATM cell payload encryption

As shown in figure 5, two physical interfaces are provided: On the one hand, the 155 Mbps synchronous transfer mode 1 (STM-1) constitutes the top level throughput. On the other hand, a 2 Mbps E1 interface is shown. This independence from the physical media is to be considered one of the main advantages of the project, as the variety of different media ATM is defined for is supported. Thus, the approach is also considered for application to satellite networks [26] and ADSL [27].

Regarding user plane confidentiality, the core unit is the key agile high-speed DES/TripleDES encryption unit (HADES). This VLSI complementary metal oxide semiconductor (CMOS) unit has been specifically designed for ATM user plane confidentiality requirements. It offers two UTOPIA compliant interfaces, one to the ATM layer component substituting a TC controller and one to the PHY layer component substituting a SAR processor. Consequently, the components interfacing to HADES are fooled a conventional ATM NIC architecture and, thus, HADES is transparent to both the SAR processor, and the TC controller, as illustrated in figure 5. Note, that figure 5 shows the two blocks 155 Mbps and 2 Mbps for concerns of illustrating the physical media independence, although just one of the two blocks can be the active one.

As ATM cells pass the encryption unit, HADES extracts the VPI/VCI pair, as well as the payload type identifier (PTI) from the ATM cell header. Spoken in exact ATM protocol model terminology, the model operates below the ATM layer. However, as the UTOPIA interface provides a start of cell (SOC) signal, the ATM cell header can be easily reconstructed from the octet stream passing the eight bit UTOPIA busses. Thus, the approach is to be considered as an ATM layer embedding of the encryption process.

The VPI, VCI information identifies the VC, whereas the PTI information identifies the ATM cell type. In the per-VC encryption approach followed, which means that each user connection (each VC) is assigned a unique session key, HADES interprets the *<VPI, VCI, PTI>* triple as the encryption context applied to the ATM cell payload. This can be an arbitrary combination of DES, TripleDES, and plaintext communication, respectively ECB and CBC operational mode for each VC and communication direction transmit or receive. Providing arbitrary combinations of encryption algorithms (DES or TripleDES) and operational modes (ECB or CBC) is referred to as algorithm agile encryption [28], robustness agile encryption respectively [29]. HADES employs on-chip session key storage and management blocks which utilise CAM techniques to identify a certain encryption context, and random access memory (RAM) techniques to store the session keys and the initialisation vectors (IVs). The CAM techniques used allow to identify the encryption context within the period the first eight octet ATM cell block is loaded via UTOPIA. This minimises the delay introduced by the encryption process to below one ATM cell period. This is worth mentioning, as this minimal additional delay does not affect the QoS parameters of the application. Actually, the latency between ATM cell data entering HADES at the input UTOPIA interface and the corresponding encrypted data leaving HADES at the output UTOPIA interface is in the magnitude of 1 μs when operating at the top level throughput of 155 Mbps which is significantly below an ATM cell period (an ATM cell period is approximately 2.8 μs at 155 Mbps STM-1).

Whereas the encryption services are implemented in hardware giving the flexibility of a robustness agile ATM encryptor, a higher degree of flexibility is required for the security context negotiation process including session key exchange and authentication. Specific user requirements, as well as legal constraints may require different key exchange methods applying different cryptographic strength in terms of key length. To decouple the encryption unit from the key exchange process, the corresponding functions are implemented in software and embedded into the operating system's kernel space, included into the drivers section of the SCAN NIC. The session keys are enclosed into specific OAM F5 section flows and, thus, ATM cells passing the UTOPIA interface are used to load an encryption context to HADES. This keeps the hardware and platform independence of the encryption unit.

The overall objective of SCAN is a secure ATM NIC fitting a single-slot peripheral component interface (PCI) bus for PCs. The drivers implemented are network driver interface standard (NDIS) version 5 supporting

Windows 2000 and Windows 98. The secure ATM NIC provides user plane confidentiality by employing HADES featuring DES and TripleDES in CBC and ECB operational mode. The physical interfaces supported are 155 Mbps STM-1 and 2 Mbps E1. End system authentication and session key exchange using 1024 bit RSA, as well as the support services utilising security IEs for UNI version 4.0, user plane blocking, and OAM flows as discussed in section 3.5 are integral part of SCAN. At the time of writing this paper, the design of HADES has been completed in a 0.6 micron CMOS process. First engineering samples and, thus, prototypes of HADES integrated into the SCAN secure ATM NIC are expected for the forth quarter of 1999.

6. CONCLUSIONS

The paper has presented a comprehensive survey on the topic of security services in ATM networks. The security requirements have been identified and the variety of different approaches has been described. The advantages and disadvantages of each approach have been discussed. In particular, implementation issues have been identified, such as applicability to state-of-the-art ATM hardware. The standardisation efforts by the ATM Forum have been outlined and, finally, the project SCAN which is streamlined to this standard has been presented.

REFERENCES

[1] I.F. Akyildiz and K.L. Bernhardt, ATM Local Area Networks, A Survey of Requirements, Architectures, and Standards, IEEE Communications Magazine v. 35, n. 7, 1997.

[2] M.H. Behringer, The Implementation of TEN-34, Proceedings of 8th Joint European Networking Conference JENC'97, 1997.

[3] URSA consortium, User Requirements and Strategies for Application, Final report of RACE project URSA, R2091, WP7, 1995.

[4] B. Khasnabish, Broadband to the Home (BTTH): Architectures, Access Methods, and the Appetite for it, IEEE Network v. 11 n. 1, 1997.

[5] L.A. Ims, D. Myhre, B.T. Olsen, Economics of Residential Broadband Access Network Technologies and Strategies, IEEE Network, v. 11, n. 1, 1997.

[6] K. Maxwell, Asymmetric Digital Subscriber Line: Interim Technology for the Next Forty Years, IEEE Communications Magazine v. 34, n. 10, 1996.

[7] E.J. Hernandez-Valencia, Architectures for Broadband Residential IP Services Over CATV Networks, IEEE Network v. 11, n. 1, 1997.

[8] M. Peyravian and T. Tarman, Asynchronous Transfer Mode Security, IEEE Network, v. 11, n. 3, 1997.

[9] ATM Forum, ATM Security Framework 1.0, The ATM Forum Technical Committee, AF-SEC-0096.000, 1998.

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

[11] ITU-T, B-ISDN Protocol Reference Model and its Application, Recommendation I.321, International Telecommunication Union, Telecommunication Standardisation Sector, 1991.

[12] G. Dobrowsky, (Ed.), ATM User-Network Interface Version 3.1 Specification, The ATM Forum, Technical Committee, 1994.

[13] M. Goguen, (Ed.), Private Network-Network Interface Specification Version 1.0, The ATM Forum, Technical Committee, 1996.

[14] U. Ellermann, C. Benecke, Firewalls for ATM Networks, Proceedings of International Congres on Information Technology Security INFOSECcom, 1998.

[15] H. Cruickshank, Z. Sun, S. Valentzas, A Proposal for Security Services in ATM Networks, Proceedings of the 4th IFIP Workshop on Performance Modelling and Evaluation of ATM Networks, 1996.

[16] J. Forné, J.L. Melús, An integrated solution for secure communications over B-ISDN, in: Communications and Multimedia Security II, ed. P. Horster, Chapman & Hall, 1996.

[17] R.H. Deng, L. Gong, A.A. Lazar, Securing Data Transfer in Asynchronous Transfer Mode Networks, Proceedings of Globecom'95, 1995.

[18] S.C. Chuang, Securing ATM Networks, Proceedings of 3rd ACM Conference on Computer and Communications Security, 1996.

[19] M. Laurent, O. Paul, P. Rolin, Securing communications over ATM Networks, in: Global IT Security, ed. L. Yngstrom, Chapman & Hall, 1997.

[20] R.J. Cherukuri, M. Peyravian, S.F. Wu, A User Plane Security Protocol for ATM Networks, Proceedings of 5th International Conference on Telecommunication Systems, 1996.

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

[22] H. Leitold, U. Payer, R. Posch, A Hardware Independent Encryption Model for ATM Devices, Proceedings of 14th Annual Computer Security Applications Conference ACSAC'98, 1998.

[23] D. Stevenson, N. Hillery, and G. Byrd, Secure Communications in ATM Networks, Communications of the ACM, v. 38, n. 2, 1995.

[24] A. Rieke, Link Encryption in ATM Systems, in: Communications and Multimedia Security III, ed. S. Katsikas, Chapman & Hall, 1997.

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

[26] H. Cruickshank, B.G. Evans, I. Mertzanis, H. Leitold, R. Posch, Securing Multimedia Services Over Satellite ATM Networks, International Journal of Satellite Communications, v. 16, n. 4, 1998.

[27] E. Areizaga, P. Ibañez, H. Leitold, R. Posch, M. Laurent, J.M. Mateos, J.L.M. Gonzá lez, Secure Communications in ATM over Access Networks, to appear in proceedings of Broadband Access Conference BAC'99, 1999.

[28] T.D. Tarman, R. L. Hutchinson, L. G. Pierson, P. E. Sholander, E. L. Witzke Algorithm-Agile Encryption in ATM Networks, IEEE Computer, v. 31, n. 9, 1998.

[29] L.G. Pierson, E. L. Witzke, M. O. Bean, G. J. Trombley, Context Agile Encryption for High-Speed Communication Networks, ACM SIGCOMM, Computer Communications Review, v. 29, n. 1, 1999.