ATM SECURITY

A Survey of Research, Products, and Standards

Extended abstract of the mini-tutorial

Herbert Leitold

Institute for Applied Information Processing and Communications (IAIK)

Graz University of Technology

Inffeldgasse 16a, A-8010 Graz, Austria

Herbert.Leitold@iaik.at

Key words: ATM security tutorial, ATM Forum Security Specification, ATM security products

Abstract: With the increasing deployment of asynchronous transfer mode (ATM) in both local area network (LAN), and wide area network (WAN) environments the interest in secure means of transferring sensitive information over ATM increases. Given potential application fields requiring Quality of Services (QoS) provided by ATM, as diverse as transferring medical images, linking branch offices to company networks, or governmental networks transferring sensitive citizen information, security is not only a desired option, it is rather an indispensable necessity.

The weakness of solutions to security in ATM networks has been recognised early. Cryptography is the tool of choice to achieve secure communications and a couple of proposals appeared to integrate cryptographic functions into ATM. Products have been developed which at the beginning faced the uncertainty of missing standards frameworks. However, this issue has been made up, as the ATM Forum has recently approved the Security Specification 1.0 which is in fact a comprehensive standardisation effort building the buttress for interoperable products.

In this tutorial, the ATM security arena is surveyed. It first gives an explanatory overview of ATM as a technology and addresses the challenges specific to ATM when aiming to migrate ATM to a secure infrastructure. Basing on these challenges, promising approaches to achieve security in ATM networks are described. By assessing the specific advantages and disadvantages, a comparison of the approaches against the ATM Forum Security Specification is made. In its final part, the tutorial surveys products

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](https://doi.org/10.1007/978-0-387-35581-8_35)

that are already available on the market or are announced by manufacturers working on ATM security.

1. INTRODUCTION

Networks based on cell relaying techniques origin from research done in the late 1970's and early 1980's as a novel approach to efficiently transport speech and video information (see [1] for a short description of cell relay history). With the first commercially available asynchronous transfer mode (ATM) switches, ATM network adaptors, and ATM local area network (LAN) solutions in the early 1990s [2], ATM gained a substantial stimulus and attracted the broad attention of numerous universities and research labs. Within less than a decade, ATM matured to a established technology in both LAN, and WAN environments, mainly because of the high bandwidth offered and the Quality of Services (QoS) guarantees.

However, almost together with the first ATM pilot installations not only the prospect of novel broadband networking applications became apparent, there have also been first rumours and concerns about security issues, as for instance expressed in a talk by Henning Schulzrinne "*ATM: Dangerous at any speed?*" [3]. In fact, ATM is as vulnerable to threats, such as wiretapping, forgery, or spoofing, as other networking technologies. What to some extent distinguishes ATM from most of the other networking technologies is, that efforts to overcome security risks have been made prior to its broad deployment.

In this mini-tutorial, security in ATM networks is discussed. Therefore, section 2 sketches the basics of ATM. The protocol reference model, as well as the principle architecture of ATM networks are addressed. In section 3, approaches to ATM security are surveyed by discussing relevant publications. An overview of standards related to ATM security is given in section 4. A survey of ATM security products is given in section 5 and, finally, conclusions are drawn.

2. ATM BASICS

Cell relaying is based on the idea of small data units of a fixed size—so-called cells—which carry a connection identifier in its header. Spoken in simple terms, the connection identifier enables efficient switching of the cells to appropriate outputs by the means of lookup tables or content

addressable memory (CAM) techniques, whereas the fixed size enables efficient buffering algorithms within the switching elements.

To associate the connection identifier to communicating end systems signalling functions are invoked upon establishing a connection—termed switched virtual connection (SVC)—or the association is fixed upon prior agreement with the network service provider—termed permanent virtual connection (PVC).

ATM promises to support the QoS required by a variety of services, such as real-time voice and video or delay insensitive data communication. Therefore, a number of ATM adaptation layers (AALs) are defined that convert the application data to the ATM cell format by invoking convergence sublayer (CS) and segmentation and reassembly (SAR) functions.

An ATM cell carries a five octet header and a 48 octet payload. The connection identifier is embedded into the ATM cell header as 24 bit virtual path identifier, virtual connection identifier (VPI, VCI) pair at the user network interface (UNI). In addition, a 3 bit payload type identifier (PTI) defines the ATM cell type, a cell loss priority (CLP) bit marks those cells that are preferably to be discarded, if this is required in network congestion periods, and a header error checksum (HEC) is provided in order to avoid misrouted cells in the case of bit errors in the header.

Beside the service independence, a major advantage of ATM is that it is defined independent from the physical media. Currently, 155 Mbps OC3c or 622 Mbps OC12c signals represent commonly used LAN end system and backbone links, whereas 1.5 Mbps T1, 2 Mbps E1, 34 Mbps E3, or 45 Mbps T3 signals for broadband WAN accesses are common. To support this broad range of signals, a physical layer embeds ATM cells to the transmission frame by employing transmission convergence (TC) and physical media dependent (PMD) functions.

Above stated characteristics represent the ATM protocol reference model [4], where the AAL interfaces to the application utilising ATM, respectively to the ATM layer which itself interfaces to the physical layer. In addition to these layers, a control plane performs the signalling to establish virtual channels (VCs), a user plane is responsible for transmitting the user data, and, finally, a management plane defines the functions to keep the network operational.

Associating the protocol reference model with the ATM network architecture, end systems at the UNI convert the user data to ATM cells by employing the AAL and transmit the bitstream resulting from the physical layer functions. The network elements—termed ATM switches—implement the signalling AAL (S-AAL, control plane) to associate end system connection requests to a VPI, VCI pair. In the user plane, ATM switches

operate at the ATM layer that mainly performs VPI, VCI translation, as in the general case these values of the header are modified whilst an ATM cell passes an ATM switch.

So how does security fit in? Given above sketched principle functioning of ATM networks, a number of threads can be identified, where some threads and user's perspectives to secure ATM communication are, as follows: By fooling the signalling procedures of the network, an end system might masquerade which results in authentic signalling, entity authentication, and data origin authentication as basic requirements. If ATM cells carrying a legitimate VPI, VCI are injected to an ingress switch, the additional data fools the receiving end system—data integrity proofs are desirable. As the ATM cells pass the network in plain text, wiretapping is possible which asks for data confidentiality. Finally, restricting the access to certain network resources asks for access control.

Cryptography is the tool of choice to meet these security requirements. In the following section of the tutorial, an overview to the research community's approaches to ATM security is given.

3. KEY PUBLICATIONS ON ATM SECURITY

In this section of the tutorial, the essentials of key publications in the ATM security arena are described, respectively an overview to common and distinct approaches is given in this abstract. For a more detailed description, the reader is guided to [5], where Donglin Liang reports on ATM security and gives a comprehensive reference list.

The references on ATM security can be categorised into two classes: Firstly, from an ATM network and service provider's viewpoint, issues such as availability, secure management, survivability, fraud, and billing are the focus. Secondly, from an end user's point of view, the major interest is in data confidentiality, authentication, data integrity, and access control. In this tutorial, the main focus is on the end user's perspectives, although the interests overlap, as availability or evading fraud are obvious user perspectives, respectively user security services constitute marketable added value for network providers.

For end-to-end security services, a possible distinction between different proposals and approaches is the embedding into the ATM protocol model. A major user perspective is that a security solution shall not counteract the benefits offered by ATM. With reference to section 2, these are QoS guarantees for different service classes and applicability to various physical media. Taking this consideration into account, embedding of security services into the ATM layer is an obvious choice, as the ATM layer is

independent from the AALs representing the different service classes, as well as independent from the physical layer. Consequently, for encrypting user data, the protocol data unit (PDU) to encrypt is the ATM cell payload. This approach raises two general challenges: Firstly, a general one in broadband networks is the high bandwidth to be dealt with. This leads to symmetrical ciphers implemented in hardware, such as the data encryption standard (DES), IDEA, or FEAL. The second challenge is ATM specific: As ATM cells are statistically multiplexed between different VCs, the requirement of having unique keys for each user connection—termed per-VC encryption—requires to change session keys rapidly between ATM cells assigned to different VCs. This is termed a key-agile encryption unit and discussed by Stevenson, et.al. in [6] and [7], the latter in fact amongst the best known publications on ATM security. Beyond that publications, in [8] a CAM-based approach to key agility is discussed. In [9], algorithm-agile encryption is introduced, where the encryption unit not just switches between keys, it even enables different encryption algorithms to be applied to different VCs. Finally, the concept of a ATM confidentiality system for 10 Gbps OC-192 is discussed in [10].

Approaches to confidentiality systems that are embedded into the AAL are discussed by Chuang [11], Deng, et.al. [12], Cruickshank, et.al. [13], and Laurent, et.al. [14]. However, these approaches face the problem that it requires an implementation for each AAL, such as one for real-time AAL-1 and one for computer-based communication using AAL-3/4 or AAL-5. Thus, the state-of-the-art is represented by above described ATM layer embedding of security services.

In addition to data confidentiality, data integrity is of importance. Therefore, message authentication codes (MAC) are appended to the PDU, respectively digital signatures are used for integrity proofs of signalling messages. At the ATM layer, the PDU is of a fixed size, i.e., the 48 octet ATM cell payload. Adding a MAC is not possible in the general case. For data integrity, embedding the MAC to the AAL is advantageous, as AAL-5 and AAL-3/4 frames are of variable size. This has been proposed by [14] respectively by Cherukuri, et.al. in [15] and Forné and Melús in [16].

For session key exchange, symmetric algorithms, such as block ciphers in cipher block chaining (CBC) operational mode, but mainly asymmetrical algorithms, such as Rivest, Shamir, Adleman (RSA) or Diffie Hellman (DH), are used for robustness and key distribution considerations. For performance reasons, symmetrical algorithms are used for re-negotiating keys in most cases, even if the initial negotiation uses asymmetrical algorithms. The relevant publications propose to either include authentication and key exchange into the signalling sequence, or to employ an in-band channel in the user plane. These approaches are discussed in

above stated publications [7], [11], and [14]. For authentication employing the same communication channels, as the key exchange protocols (user plane and control plane), established standards on digital certificates—mainly X.509—are used, as discussed in [12], respectively by Shankaran and Varadharalan in [17] who also discuss access control issues.

An overview to the ATM security services addressed in this section is given by Peyravian and Tarman [18] who both have been engaged as founder and chairpersons in the ATM Forum Security Working Group. This leads to the standardisation arena, which is discussed in the following section.

4. ESTABLISHED STANDARDS

In this section of the tutorial, relevant ATM security standards are discussed. These standards result from the efforts made by the ATM Forum to define normative references to migrate ATM to a secure infrastructure and are sketched in the following subsections.

4.1 ATM Forum Security Framework 1.0

In the Security Framework 1.0 [19], the ATM Forum defined ATM security objectives, identified threads, and derived general security requirements and services for ATM networks. This resulted in ten guiding principles, as follows (citations taken from [19]):

- AF SEC-1: The ATM network shall support capabilities to establish and verify the claimed identity of any actor in an ATM network (verification of identities).*
- AF SEC-2: The ATM network shall support capabilities to ensure that actors are prevented from gaining access to information resources they are not authorised to access (controlled access and authorisation).*
- AF SEC-3: The ATM network shall support the capability to keep stored and communicated data confidential (protection of confidentiality).*
- AF SEC-4: The ATM network shall support granting the integrity of stored and communicated data (protection of data integrity).*
- AF SEC-5: The ATM network shall support the capability that an entity can not deny the responsibility for any of its performed actions as well as their effects (strong accountability).*

- AF SEC-6: The ATM network shall support capability to retrieve information about security activities stored in the Network Elements with the possibility of tracing this information to individuals or entities (activity logging).*
- AF SEC-7: The ATM network shall support the capability to generate alarm notifications about certain adjustable and selective security related events (alarm reporting).*
- AF SEC-8: The ATM network shall support the capability to analyse and exploit logged data on security relevant events in order to check them on violations of system and network security (audit).*
- AF SEC-9: The ATM network shall support recovery from successful and attempted breaches on security (security recovery, management of security).*
- AF SEC-10: The ATM network shall support capabilities to manage the security services derived from the security requirements listed above (security recovery, management of security).*

In addition to above listed requirements, the ATM Forum Security Framework gives a plane specific interpretation of the ten security requirements. Basing on this framework, the ATM Forum Security Specification 1.0 [20] has been defined, which is sketched in the following subsection.

4.2 ATM Forum Security Specification 1.0

As a comprehensive standards effort to enable interoperable ATM security solutions, the ATM Forum Security Specification 1.0 [20] has been recently approved in its February 1999 version. It defines security services for the control plane, the user plane, and support services, as follows:

- **Control plane:** The specified security services are data origin authentication, data integrity, and the impact of error conditions such as incompatible signalling channel endpoints. Thus, the specification's scope is authentication and data integrity of ATM signalling in a hop-by-hop manner between adjacent signalling entities.
- **User plane:** For the user plane, entity authentication, confidentiality, data origin authentication, data integrity, and access control are defined. This results in a comprehensive normative reference to secure end-system communication.
- **Support services.** The support services define the protocols and for security information exchange, the key exchange functions, session key update protocols to renew negotiated session keys, respectively states

that X.509 shall be used for certificate exchange in the signalling channel or in-band in the user plane.

The specification defines a number of algorithm profiles for authentication, confidentiality, and data integrity. The cryptographic algorithm options employed are: DES, Triple-DES and FEAL in CBC or a counter operational mode are defined for data confidentiality. DES/CBC, FEAL/CBC digital signature algorithm (DSA), ESIGN, elliptic curve DSA-like, RSA signatures with secure hash algorithm (SHA) or message digest 5 (MD5) hash functions are employed for authentication and data integrity. For key exchange DES/CBC, TripleDES/CBC, FEAL/CBC, DH, RSA, and elliptic curve DH are defined, and finally, the message authentication codes that have been specified are DES/CBC, FEAL/CBC, MD5, and SHA.

4.3 UNI 4.0 and PNNI 1.0 Security Signaling Addendum

The ATM Forum Security Specification 1.0 defines additional signalling information elements (IEs) for carrying out support services in the control plane. These IEs are defined as a security addendum to the related signalling standards UNI 4.0 [21] and private network-network interface (PNNI) version 1.0 [22].

5. PRODUCT OVERVIEW

In its final section, the tutorial discusses different market available ATM security products, as well as recent product announcements. Although to some extent similar in its main characteristics and mainly oriented towards the ATM Forum Security Specification, each has interesting specific features which are outlined in the tutorial. The surveyed products are: Cyphercell™ [23] is a comprehensive implementation of the ATM Forum specification for 155 Mbps OC3c and currently under evaluation for the Common Criteria EAL4 security rating. HC-7910™ [24] is a key-agile encryptor that features a variety of physical interfaces and employs a proprietary encryption algorithm. In addition to being an ATM encryption unit, the ATLAS™ [25] series for OC3c has firewall functions employing a patented policy cache architecture. Again for OC3c, the Cylink ATM Encryptor [26] is a key agile unit. A National Security Agency (NSA) certified Type 1 encryptor capable of up to 622 Mbps OC12 is the unit FastLANE™ [27]. Featuring a number of physical interfaces up at 155 Mbps OC3c with a 622 Mbps OC12c

physical interface announced for fourth quarter of 1999 is the key agile encryption unit CellCase™ [27].

Above stated products have in common, that each is a line intercepting unit that is typically installed between an ATM end system or ATM switch and the ingress switch of the network service provider. The author of this paper is involved in the project Secure Communication in ATM Networks (SCAN) [28]. This project is embedded into the Advanced Communications and Services (ACTS) Programme of the European Commission. The SCAN objective is to bring ATM security services to the desktop by integrating a key agile high-speed ATM DES/TripleDES (HADES) unit to a 155 Mbps ATM network interface card for PCs.

6. CONCLUSIONS

In this paper the mini-tutorial on ATM security has been abstracted. In order to prepare for its major contents, the basics of ATM have been sketched and potential security threads have been identified. This has been followed by giving an overview to recent research related to ATM security and by outlining different approaches. Relevant standards that have been defined by the ATM Forum have been addressed and the extended abstract has been completed by giving a short survey of products that are established in the market.

REFERENCES

- [1] Cell relay frequently asked question, Who is the inventor of ATM?, subject G4 <http://cell-relay.indiana.edu/cell-relay/FAQ/ATM-FAQ/g/g4.htm> , 1997.
- [2] E. Biagioni., E. Cooper., R. Sansom, Designing a Practical ATM LAN, IEEE Network, v. 7, n. 2, 1993.
- [3] H. Schulzrinne, ATM: Dangerous at any Speed?, Proceedings of IEEE Gigabit Networking Workshop GBN'95, 1995.
- [4] ITU-T, B-ISDN Protocol Reference Model and its Application, Recommendation I.321, International Telecommunication Union, Telecommunication Standardisation Sector, 1991.
- [5] D: Liang, A Survey on ATM Security, student report, Ohio State University, Computer and Information Science Department, 1997. online available at: http://www.cis.ohio-state.edu/~jain/cis788-97/atm_security/
- [6] D. Stevenson, N. Hillery, G. Byrd, F. Gong, D. Winkelstein, Design of a Key Agile Cryptographic System for OC-12c Rate ATM, Proceedings of Internet Society Symposium on Network and Distributed Systems Security, 1995.
- [7] D. Stevenson, N. Hillery, and G. Byrd, Secure Communications in ATM Networks, Communications of the ACM, v. 38, n. 2, 1995.

- [8] 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.
- [9] 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.
- [10] 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.
- [11] S.C. Chuang, Securing ATM Networks, Proceedings of 3rd ACM Conference on Computer and Communications Security, 1996.
- [12] R.H. Deng, L. Gong, A.A. Lazar, Securing Data Transfer in Asynchronous Transfer Mode Networks, Proceedings of Globecom'95, 1995.
- [13] 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.
- [14] M. Laurent, O. Paul, P. Rolin, Securing communications over ATM Networks, in: Global IT Security, ed. L. Yngstrom, Chapman & Hall, 1997.
- [15] 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.
- [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. Shankaran, V. Varadharajan, Secure Signalling and Access Control for ATM Networks, Proceedings of 14th Annual Computer Security Applications Conference ACSAC'98, 1998.
- [18] M. Peyravian and T. Tarman, Asynchronous Transfer Mode Security, IEEE Network, v. 11, n. 3, 1997.
- [19] ATM Forum, ATM Security Framework 1.0, The ATM Forum Technical Committee, AF-SEC-0096.000, 1998.
- [20] ATM Forum, ATM Security Specification, Version 1.0, ATM Forum Technical Committee, ATM-SEC-01.0100, 1999.
- [21] ATM Forum, UNI Signaling 4.0 Security Addendum, ATM Forum Technical Committee, ATM-CS-0117.000, 1999.
- [22] ATM Forum, PNNI Version 1.0 Security Signaling Addendum, ATM Forum Technical Committee, ATM-CS-116.000, 1999.
- [23] CATM, CIPHERCELL™, online information at: <http://www.ctam.com.au/>
- [24] Cellware Broadband & Crypto AG; HC-7910 ATM Encryptor, online information at: <http://www.crypto.ch/>
- [25] StorageTek®, ATLAS 2002 and 2003 ATM Line Access and Security System, online information at: <http://www.stortek.com/StorageTek/network/NetSentry/ATLAS/>
- [26] Cylink, Cylink ATM Encryptor, online information at: <http://www.cylink.com/>
- [27] GTE, FASTLANE®, <http://www.gte.com/Products/Prods/fastlane2.html>
- [28] Celotek, CellCase, online information at: <http://www.celotek.com/>
- [29] SCAN, Secure Communication in ATM Networks, European Union, DXII funded ACTS project AC330, <http://www.iaik.tu-graz.ac.at/Research/SCAN/>