A User Plane Security Protocol for ATM Networks

Rao J. Cherukuri, Mohammad Peyravian
Venkata Surapaneni

IBM Corporation
P.O.Box 12195
RTP, NC 27709
{raoc, peyravn, vsurapaneni}@vnet.ibm.com

Shyhtsun F. Wu[*]

Computer Science Department
North Carolina State University
Raleigh, NC 27695
wu@csc.ncsu.edu

October 9, 1996

Abstract

Asynchronous Transfer Mode (ATM) has been identified as the transfer mode for implementing *Broadband ISDN (BISDN)*, a universal network supporting different applications and customer categories. Many of these applications involve sensitive data or highly valuable information flows. Therefore, network security is one critical issue in offering ATM services. In this abstract, we first analyze the security requirements for ATM networks and identify the secure ATM protocol stack. Then, we propose a simple solution to enhance the user-plane security of ATM networks. Our solution utilizes the existing ATM signaling protocol (*e.g.,* OA&M F5 cells) to exchange security management information like session keys and re-synchronization tokens. We also map and integrate a simple session key exchange protocol into the existing ATM call-setup protocol.

[*]Supported in part by the U.S. Department of Defense Advanced Research Projects Agency and the U.S. Air Force Rome Laboratory under contract F30602-96-C0325, and in part by the Center for Advance Communication and Computing under grant FAS #5-30183.

1 Introduction

Asynchronous Transfer Mode (ATM) has been identified as the transfer mode for implementing *Broadband ISDN (BISDN)*, a universal network supporting different applications and customer categories. Many of these applications involve sensitive data or highly valuable information flows. Therefore, network security [Chu95, SHB95, DGL95] is one critical issue in offering ATM services.

Many organizations are studying security solutions for ATM. Chuang[Chu95]) considered what cryptographic tools or protocols are necessary to offer these security services. The MCNC group [SHB95] built secure ATM switch prototypes with Digital's DES chips [Ebe92] to support *link encryption*. The ATM forum technical committee [PH95, PTH95] is currently developing a security architecture [ATM96] for ATM networking services. The ATM specification draft, which is still in progress, divides the security problem into *User plane security* (end to end or switch to switch), *Control and Management plane security*, and *Access control*.

What we do not have yet is a simple and practical solution that can be easily integrated into the existing ATM framework and even maybe an existing ATM network. Or, at the very least, it is desirable to develop a low-cost upgrade process for secure ATM services. In this paper, we propose a simple user-plane security solution building on top of existing ATM services. In the next section, we briefly provide some background information about ATM. Then, we discuss the security requirements. Finally, we propose our solution for these requirements.

2 ATM Background

The ATM protocol reference model consists of three planes: user plane, control plane and management plane. Each plane is modeled as a separate entity based on OSI protocol reference model. One of the differences between ATM and conventional protocols like X.25 and TCP/IP is that conventional protocols include control signaling on the same channel as data transfer, whereas ATM uses a common channel signaling which is separate from data transfer channel. The Operations Administration and Maintenance (OAM) of the ATM connections is a part of the management plane, which performs coordination functions related to both the user plane and control plane. The functions includes performance monitoring, defect and failure detection, fault localization and system management.

The ATM protocol reference model consists of *physical layer, ATM layer, ATM Adaptation layer (AAL)* and Higher layers. The logical connections in ATM are referred to as Virtual Channels (VCs). A VC is analogous to a X.25 virtual circuit or a Frame Relay connection. A Virtual Path (VP) is a bundle of VCs that have the same end points. The ATM virtual connections can be provisioned using network management. These connections are called Permanent Virtual Channels (PVC). Further, the virtual channels can be dynamically established using ATM signaling procedures. These virtual channels are called Switched Virtual Channels (SVCs).

3 User Plane Security

The user plane security deals with security for VCs established between the end users. As other types of networks, the end to end user plane VC security involves support of the following requirements:

Authentication: Supports authentication of the user plane entities.

Confidentiality: Supports confidentiality for VCs which is concerned with prevention of eavesdropping.

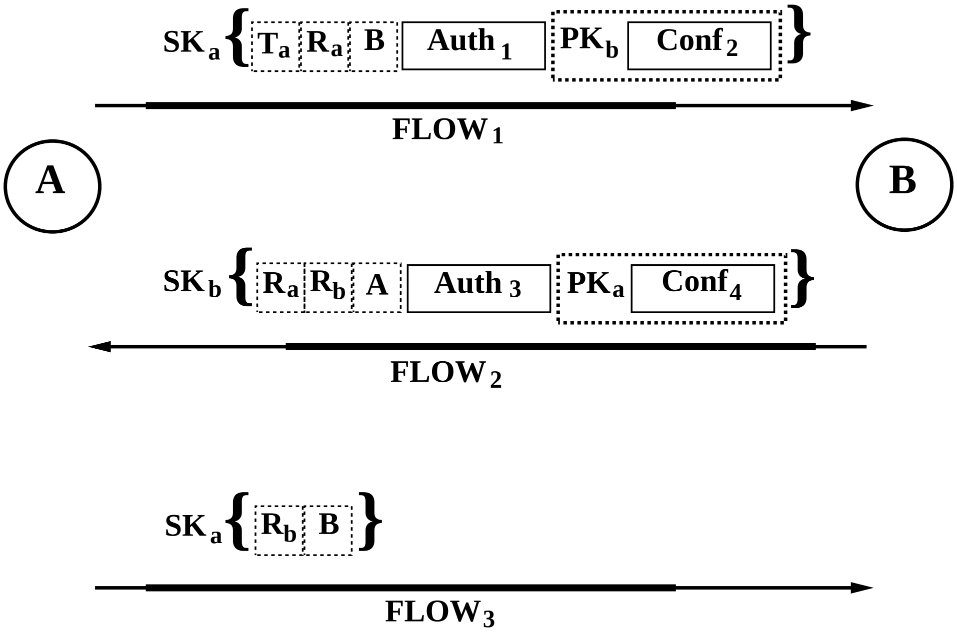

Figure 1: Mutual Authentication Flows

Data integrity: Supports data integrity for VCs which is concerned with detecting efforts to altered data.

In this section, we briefly describe how these security requirements can be fulfilled in ATM networks.

3.1 Authentication

Authentication requires that the entity be authenticated to have a distinguished name (ID) and an associated key. Entities in ATM can be identified using two address formats: NSAP format (private address format);. E.164 format. The NSAP format has fixed length for the address whereas the E.164 format has variable length addresses. The ATM Forum specifies the use of NSAP format to identify the ATM entities. The addresses are 20 bytes long.

For asymmetric (Public) key based scheme, it is assumed that each entity x has a public/private key (PK_x, SK_x) pair and knows its partners public key. The following symbols and abbreviations are used for key exchange: PK_x : The public component of X's asymmetric key. SK_x : The private component of X's asymmetric key. $Auth_1$ and $Auth_2$ in the flows are authentic parameters (parameters that require integrity protection). $Conf_1$ and $Conf_2$ are authentic and confidential parameters, i.e., parameters that require both integrity and confidentiality protection. In Figure 1, a three pass protocol is depicted for mutual authentication between two entities A and B. Please note that $Flow_3$ may be optional and a two flow protocol is described in the full paper.

3.2 Confidentiality

One critical concern for encryption in high-speed networks is performance [Zor94]. Performing encryption/decryption at the ATM cell level is straight forward because of fixed size cells. This is because the ATM cell data payload (48 bytes) divides neatly into encryption blocks. For example, one ATM cell can carry 6 DES blocks. On the other hand, the implementation of data confidentiality at the AAL layer is difficult because of variable length frame sizes and different types of AAL.

In ATM networks, secret keys for encryption schemes like DES have a short life. As indicated in [Chu95], if a key is never used for more than 10^9 cipher blocks, then the lifetime is about 10 seconds for applications like HDTV transmission. Therefore, it is important to have a secure protocol for key exchanges and re-synchronization.

Many encryption modes have been studied for ATM networks, while either *ECB (Electronic Code Book)* or *CBC (Cipher Block Chaining)* mode will be the default mode. Both ECB and CBC are robust when cells (cipher text) are lost. Lossing a cell in ECB implies lossing 6 DES blocks, while in CBC it implies 7 DES blocks. However, ECB is vulnerable to traffic and statistic analysis, while CBC can not be parallelized. The *OFB (Output FeedBack)* mode, which is essentially a secure random number generator plus exclusive-OR, is both secure and parallelizable but very sensitive to cell loss. It is still an open problem to have a chaining mode which is secure, scalable and robust.

3.3 Integrity

With ATM monitoring tools like *Attila* [SHB95], an attacker can modify, replay, or disorder the cells. It is thus important and useful to have an end-to-end integrity check at the AAL level. It is expensive to implement this integrity check at the ATM layer. First, by including *message authentication code (MAC)* information in each cell, we increase the cell processing overhead, and decrease the cell payload. For example, if MD5 [Tou95] is used, every cell is attached with a 128 bits signature. So, we loss immediately one third of the payload, or each cell can only carry 4 DES blocks. Second, the AAL layer integrity check must be done anyway because some attacks (like disorder) can not be easily detected in the ATM layer. Like in confidentiality, the integrity mechanism also requires key update synchronization.

3.4 Placement of the Security mechanism

The ATM layer is common to all types of traffic, while the AAL layer is for different types of applications. It is very desirable to provide encryption functions above the ATM layer because it will accommodate all kinds of user traffic (e.g. voice, data, and video) and security requirements. For example, we might have no encryption[1], EBC, CBC or others. Depending on the nature of the applications, the user will decide the security requirements for each virtual connection.

Since a message is divided into ATM cells, it is not feasible to provide data integrity checks at the ATM layer. Integrity can be verified either at the AAL layer or above. Different AALs are used for different service classes. Therefore, if we perform integrity checks in the AAL layer, it requires modification of several AAL formats, which is not desirable. Thus, it is proposed to support integrity by providing integrity checking above the AAL layer. With the proposed security placement, we get a protocol stack for secure ATM networking in Figure 2.

4 Authentication and Key exchange

ATM provides two types of connections: Permanent Virtual Connections (PVCs) and Switched Virtual Connections (SVCs). PVCs are established using network management procedures whereas the SVCs are established using signaling protocols. ATM security mechanisms exchange keys on a per connection basis. For SVCs, authentication and key exchange are provided during call setup. The Q.2931 messages SETUP and CONNECT are used for this purpose. In case of PVCs, there are no signaling messages

[1]Some applications do not need encryption. Some applications can NOT use certain export-control encryption schemes. For example, if an entity in US would like to talk to an entity in Europe, they must not use those encryption schemes.

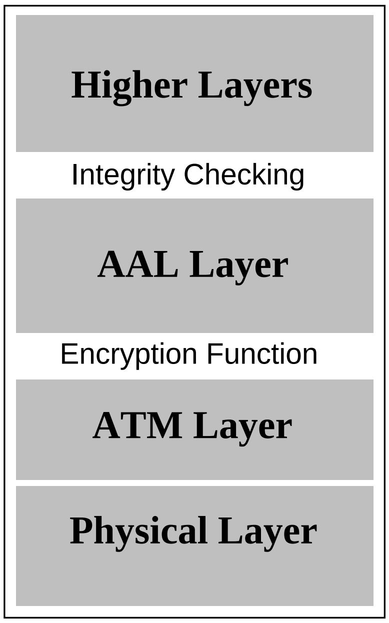

Figure 2: Protocol Stack for Secure ATM Networking Services

exchanged between the two end users. So it is not possible to use the same mechanisms that are used in SVCs for authentication and key exchange. Furthermore, there are no code points left in the ATM header (i.e. PTI field) to distinguish security information exchange from the user data at the ATM layer. So we need another mechanism to provide the security information exchange for PVCs in the user plane. Finally, temporal relation between security messages and user traffic has to preserved. Without temporal relation the communicating users will be in inconsistent states and eventually loose connection.

In the management plane, two flows are defined at the ATM level for the management of the connections. These flows are carried in the *Operations , Administration and Maintenance (OA&M)* cells. The flows at the ATM level are called as F4 and F5 flows. The F4 flows are used for Virtual Path Connections (VPCs) whereas F5 flows are used for Virtual Channel Connections (VCCs). Since end user to end user data flow uses VCC it is decided to use F5 flows for exchange of security mechanisms end to end. In addition, it can be also be used to periodically update the keys. Currently, no additional messages are defined in ATM signaling to change the keys during the life of a SVC call. So, it is proposed to use OA&M mechanism for exchange of keys during the life of the SVC call.

4.1 Exchange of Security messages using F5 OA&M cells

The F5 OA&M cells are end user to end user and the flows are bi-directional. The OA&M cell format is shown in Figure 3. The OA&M cell type field indicates the type of management function performed by the OA&M cell. Currently four types of OA&M cells are defined: fault management, performance management, activation/deactivation and system administration. The function type field indicates the function performed by the OA&M cell within the management function. The function specific field carries the information related to the function of the OA&M flow. The error detection code (EDC) field carries a CRC-10 error detection code computed over the cell data payload excluding the EDC field.

End-to-end F5 flows are terminated at the endpoints of a VCC and are passed unmodified by all intermediate nodes. The F5 OA&M cells follow exactly the same physical route as the user's data cells of

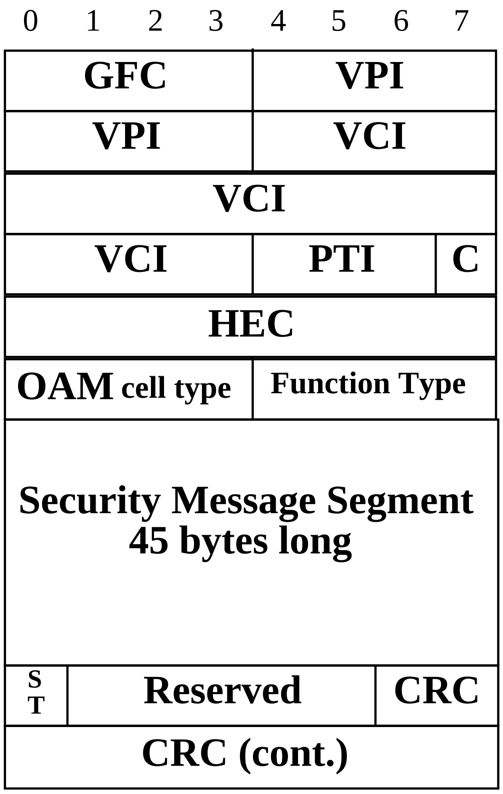

Figure 3: OA&M-F5 Cell Format at UNI

the VCC. These F5 OA&M cells have the same VPI/VCI values as the users data and are differentiated from user data by pre-assigned code-points in the payload type identifier (PTI) field in the ATM header. The PTI value = 5 (coded 101) is used for end to end F5 flows. This is called *in-band messaging* and allows temporal ordering of the messages so that the end users will be in a consistent state.

4.2 In-band Security Messages with F5 OA&M Cells

OA&M cells are used to provide the capabilities to transfer variable length security messages in-band within the data channel through the ATM network. OA&M cell based security messaging is based on AAL5 which provides non-assured delivery of security messages with length ranging from 1 to 65535 bytes. To deliver the variable length security messages in-band within the data channel, the security message is segmented into fixed size fragments so that they fit into function specific field of the OA&M F5 cells. The receiver reassembles them to get the message.

The segmentation and reassembly of OA&M cells is performed using a simplified version of AAL5 without CRC-32. The AAL5 utilizes ATM User to User indication in the PTI field of ATM header to indicate end of the message. This feature is not present in OA&M cells. In order to provide the indication of the end of message, we propose to use one bit in the reserved field of OA&M cell. The security message is appended with two bytes of length field and padding so that the total is a multiple of 45 bytes. This new message is called Protocol Data Unit (PDU). The length field tells the receiver how much is the data in the message. The PDU is segmented by the Segmentation and Reassembly (SAR) function in AAL into segments of 45 bytes. Each segment is then inserted into the function specific field of the OA&M cell. To define the PDU type, one bit can used from the reserved field in the OA&M cell. For the cell that carries the last PDU segment this bit is coded as 1 and for the remaining segments is

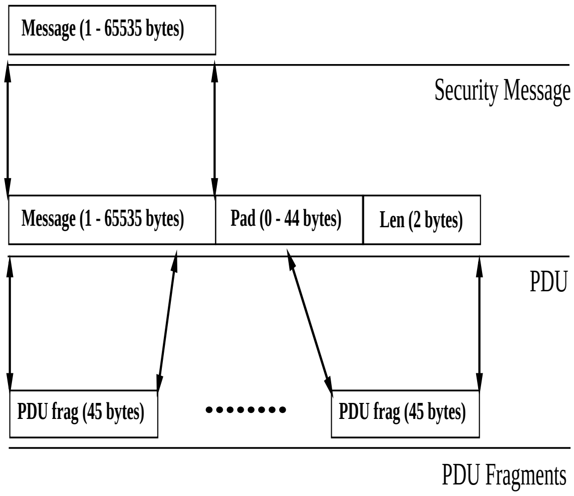

Figure 4: Segmentation and Reassembly of Security Messages

coded as 0. This process is shown in Figure 4.

A code point for function type within the system management (1111) OA&M cell to distinguish OA&M cells that carry security messages from other OA&M cells has to defined by the standard body. Currently no code points are defined for function type under system management. The OA&M cells are then transmitted using F5 (end to end) flows. The receiver relies on 10 bit CRC, the length field and "ST" bit to reassemble the PDU fragments. The 10 bit CRC covers only a single OA&M cell and does not provide protection against miss insertion from different OA&M streams or alteration of PDU segments.

4.3 Message Flows for In-band Key Exchange

As shown in Figure 5, a three-pass, RSA/nonce-based scheme is used for key exchange. The OA&M cells like any user data cells are subject to loss in the networks. The corrupted OA&M data units are also discarded by the receiving ATM entity. If the OA&M cells which are carrying the key exchange information are lost, we need to restart the whole key exchange process. Therefore, to protect the loss of $Flow_1$, we proposed to use an acknowledgment timer. The timer is stopped when $Flow_2$ is received by A. If the timer expires before $Flow_2$ arrives, the sender will resend the key using a new R_a and discards any flows that arrive and contain the old R_a.

5 Authentication and Key exchange for SVCs

Q.2931 signaling procedures are used for establishing point to point SVC connections. For point to point, the end to end messages include SETUP, and CONNECT messages [DL95] as shown in Figure 6. The other messages like CALL PROCEEDING and CONNECT ACK are of local significance. The signaling messages are identified by Call Reference and are protected using supervisory timers. When the timer expires, the call will be terminated if there is no response. This capability provides freshness and uniqueness for the signaling messages. For SVCs, it is proposed to use authentication and key exchange $Flow_1$ to be included in the SETUP message and $Flow_2$ in the CONNECT message. If the called user requests the $Flow_3$ by setting a flag in the CONNECT message, it will be send using the optional CONNECTION AVAILABLE message. The information elements will be the similar to the one's used in the OA&M flows. The details of our security modifications to the messages like CONNECT

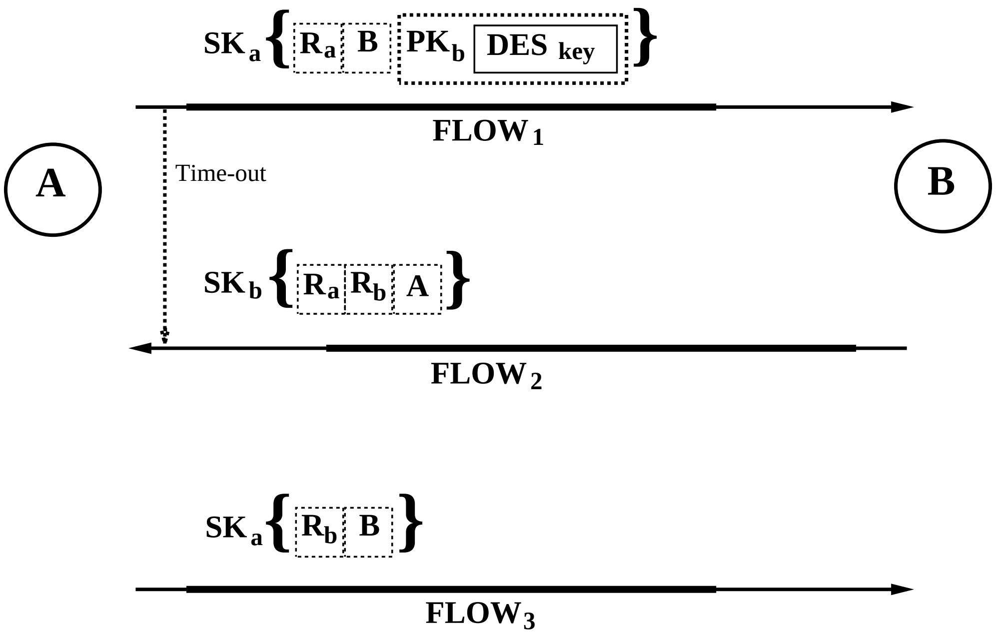

Figure 5: Message Flows for Key Exchanges

and SETUP as well as point to multiple-points security issues are included in the full paper.

6 Conclusions

In this paper, we propose a simple solution to enhance the user-plane security of ATM networks. We are currently working on control and management plane as well as access control for ATM security. Our solution presented here utilizes the existing ATM signaling protocol (*e.g.,* OA&M F5 cells) to exchange security management information like session keys and re-synchronization tokens. We also map and integrate a simple exchange protocol into the existing call-setup protocol. Another contribution is to identify the ATM security protocol stack (Figure 2). We are currently in the process of submitting our solution to the ATM forum.

References

[ATM96] Phase I ATM Security Specification (Draft). ATM Forum/95-1473R2, April 1996.

[Chu95] Shaw-Cheng Chuang. Securing ATM Networks. http://www.cl.cam.ac.uk:80/, October 1995.

[DGL95] R.H. Deng, Li Gong, and A. Lazar. Securing Data Transfer in ATM Networks. In *IEEE Global Telecommunications Conference*, Singapore, November 1995.

[DL95] H.J.R. Dutton and P. Lenhard. *Asynchronous Transfer Mode (ATM): Technical Overview*. Prentice Hall, 1995.

[Ebe92] Hans Eberle. A High-Speed DES Implementation for Network Applications. Technical Report 90, DEC SRC, Palo Alto, CA, September 1992.

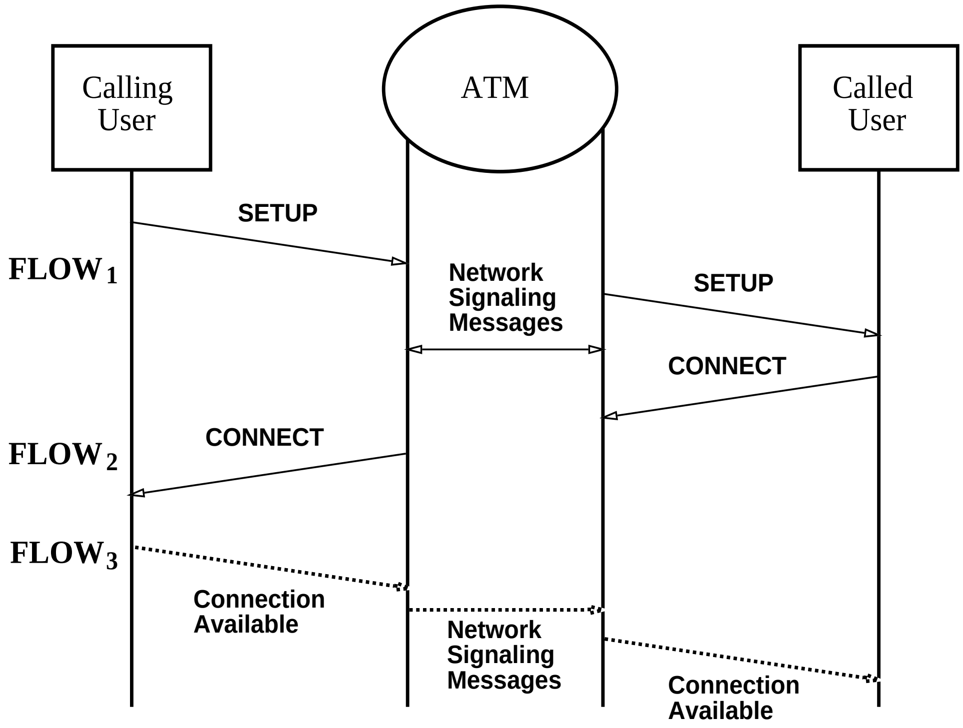

Figure 6: Connection Establishment for End-to-End Security

[PH95] Mohammad Peyravian and Els Van Herreweghen. ATM Security Scope and Requirements. ATM Forum/95-0579, June 1995.

[PTH95] Mohammad Peyravian, Gene Tsudik, and Els Van Herreweghen. A Framework for Authenticated Key Distribution in ATM Networks. ATM Forum/95-0580, June 1995.

[SHB95] D. Stevenson, N. Hillery, and G. Byrd. Secure Communications in ATM Networks. *Communications of the ACM*, 38(2):45–52, February 1995.

[Tou95] Joseph Touch. Performance Analysis of MD5. In *SIGCOMM: Communications Architectures, Protocols and Applications*, pages 77–86, Cambridge, MA, September 1995.

[Zor94] Vasilios Zorkadis. Security versus Performance Requirements in Data Communication Systems. In *Computer Security - ESORICS 94*, pages 19–30, Brighton, UK, November 1994.