Secure Communications in ATM Networks

Maryline Laurent, IRISA
Ahmed Bouabdallah, Christophe Delahaye, ENST de Bretagne
Herbert Leitold, Reinhard Posch, IAIK
Enrique Areizaga, Fundacion Robotiker
Juàn Manuel Mateos, Inelcom Ingeniera

Abstract

The ATM Forum international consortium recently approved the first version of its security specifications aiming to protect communications over Asynchronous Transfer Mode (ATM) networks by offering data confidentiality, partners authentication, etc. This paper describes the architecture of one of the first ATM Forum compliant security prototypes being currently developed in the European project SCAN (Secure Communications in ATM Networks). Additionally to the security management functions specified by the ATM Forum to exchange encryption keys and negotiate security services, SCAN implements the possibility for end-users to modify the data flow encryption algorithm during a connection in progress, and the possibility to keep the encryption algorithm choice confidential. Moreover a flexible implementation is offered allowing future users to develop their own security protocols and their own ATM security monitoring applications.

1. Introduction

The Asynchronous Transfer Mode (ATM) technology success is due to its ability to support multimedia applications needs offering high bit rates and real time guarantees. Another ATM interesting feature is the early introduction of security services into ATM specifications, thus resulting in an efficient security solution to protect the ATM traffic against eavesdropping, traffic tampering, and masquerade. The introduction of the confidentiality, integrity, and authentication services into ATM appears helpful for the deployment of security sensitive multimedia applications such as the telemedecine applications where patient files are expected to be kept confidential, and modified only by authorized persons **[1]**.
This paper describes the architecture and choices elected in project SCAN (Secure Communications in ATM Networks) to develop a prototype ensuring ATM traffic encryption at 155 Mbps, with inherent security management. This prototype is expected to be at least ATM Forum compliant, offering data encryption on a connection basis, and allowing security information to be exchanged through ATM signaling. The prototype is limited to point-to point communications environment, and additionally to the ATM Forum specifications, it implements the possibility to modify the data encryption algorithm during a connection in progress, and to improve the security level by maintaining security sensitive information secret.
This paper focuses mainly on security management aspects detailing the solutions chosen for updating session keys, and for negotiating the security services and mechanisms that will be used to protect subsequent exchanges. Attention is paid to describe the open interfaces of the prototype, which provide flexibility so that future users can develop their own security protocols fitting their own security needs, and national legislation.
More precisely, section 2 introduces ATM and the ATM security needs allowing readers to understand the remainder of the paper. Section 3 describes the security services and functions specified in current ATM Forum specifications. The following sections give a SCAN technical description, presenting the data encryption mechanism (section 4), the session key update (section 5), the security parameters negotiation (section 6), and the signaling protection (section 7). The security parameters monitored by users are presented in section 8 as SCAN security policy. The architecture of the SCAN prototype is provided in section 9, along with its open interfaces in section 10. Finally, section 11 gives some conclusions, and section 12 a list of useful acronyms.

2. Introduction to ATM security

The ATM technology is connection-oriented, that is, prior to any data exchange, it is necessary to set up connections (or virtual channels) over which data are