An Architecture for Securing Communication over ATM Network

XUN YI, EIJI OKAMOTO
School of Information Science
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Tatsunokuchi, Nomi, Ishikawa, 923-1292
JAPAN

Abstract: - The trend towards ATM network requires re-examination of network security issues. In this paper, a new architecture for securing communication over ATM networks is proposed. In the architecture, securing ATM communications can be carried out in three following stages: (1) rapidly authenticating signalling messages (such as SETUP and CONNECT) by inserting optimized security information elements into them; (2) negotiating a security context in the user plane; (3) applying negotiated security services on the user data exchange. *IMACS/IEEE CSCC'99 Proceedings,* Pages:1101-1104

*Key-Words:*ATM network,QoS,Block cipher,Public-key cryptosystem,Negotiation,Authentication.

1 Introduction

To suit the near future needs of multimedia services in terms of Quality of Service (QoS), ITU-T defined the Broadband Integrated Services Digital Networks (B-ISDN) and adopted the Asynchronous Transfer Model (ATM) as the technology to implement B-ISDN. ATM is based on the concepts of switched virtual connections and fixed length cells, this contrasts with the connectionless, shared medium, broadcast networks frequently referred to as «legacy network». These conceptual differences required the development of new protocols like «Integrated Local Management Interface» (ILMI) and «Privacy Network-to-Network Interface» (P-NNI). The specifications have not yet been subjected to a thorough security analysis.

Contributions to the ATM Forum [1] [2] [3] [4] emphasized the importance of security in ATM networks. In June 1996, the ATM Forum has published the "Phase I ATM Security Specification". This is the first step in providing clear procedure for implementing security services in ATM networks. Although some ATM specification /standard are still unavailable, ATM facilities emerge. However, current ATM facilities (e.g. ATM switches) have many restrictions which are not favorable to simple and reliable security services introduction. In addition, different countries have different rules and regulations about security issues, for example, in France any type of encryption is not allowed for transmission over public networks, in USA the official encryption method for business data is the Digital Encryption Standard (DES) with 56 bit long key. The obstacle prevented the progress of security deployment in ATM networks.

Therefore, any architecture for securing communications over ATM networks must be compliant with restrictions implied within ATM networks. In the same time, it must be flexible to allow rapid implementation of various encryption methods and key lengths so as to be approved by various government. Also, it must be able to adapt security service to each country regulation to allow international communication.

Some works for introducing security services into ATM Protocol Reference Model were done in [5] [6] [7] [8] [9]. Based on differences between the methods for negotiating a security context, they can be divided into three sorts:

(1) negotiation through signalling information;
(2) negotiation through management information;
(3) negotiation through an auxiliary channel.

According to distinctions between the methods for securing user data exchange, they can be divided into three sorts:

(1) confidentiality at the higher layer;
(2) confidentiality in the ATM layer;
(3) confidentiality in the AAL layer.

All of the solutions include more or less drawbacks. In this paper, we proposed a new architecture for securing communication over ATM networks. In the architecture, securing ATM communications can be carried out in three following stages:

(1) rapidly authenticating signalling messages (such as SETUP and CONNECT) by inserting optimized security information elements into them;

(2) negotiating a security context in the user plane;

(3) applying negotiated security services on the user data exchange.

2 Description of the Architecture

Since securing ATM communications in our architecture is based on firstly authenticating signalling messages, secondly negotiating a security context and finally applying negotiated security services on the user data exchange, the solution's description can be divided into three corresponding subsections. Throughout these sections, notations are listed as follows:

A	Calling entity
B	Called entity
CA, CA'	Certificate authority entities
Cert_CA (A)	A's certificate generated by CA
$K_{SA}(M)$	Encrypted M with A's private key
$K_{PA}(M)$	Encrypted M with A's public key
T_A	Time stamp generated by A

Table 1 Notations

To illustrate the security services and threats in ATM networks, we will refer to the following security model in ATM environment throughout this paper.

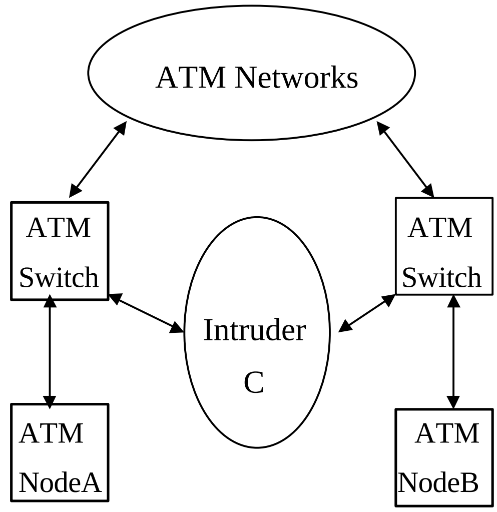

Figure 1 Security model of ATM communications

2.1 Authenticating Signalling Message

In ATM network, control plane security specification for authentication of endpoint communications is one of important issues addressed in «*Phase I ATM Security Specification*». Security-related contributions by Xerox [2], Sandia [3] and Bellcore [4] all address the issue of security signalling in ATM network.

As far as the model (**Figure 1**) is concerned, when the node A (calling entity) needs to set up a connection to the node B (called entity), A will need to send *SETUP* message to B. If this is done in the clear (no authentication), the C (the intruder) can inject *RELEASE* or *RESTART* message using the call reference number from A's *SETUP* message, causing the closing of the VC connection. This is an example of access denial to the network.

In addition, ATM network is a kind of high speed network. It is very important to reduce the latency of the authentication protocol run. The length of such protocol run will cause an impact on the call setup performance, which is a key quality of service indicator that a network service provider can provide to customer.

Therefore, rapidly authenticating signalling message is desirable for security services in ATM networks.

Our proposal authenticates signalling messages by inserting security information elements in signalling message. The security information elements are as follows:

(1) *Cert_CA(A)*, $E_{SA}(T_{A,}B)$ within signalling messages for calling entity A;

(2) *Cert_CA'(B)*, $E_{SB}(T_{B,}A)$ within signalling messages for called entity B.

where $Cert\_CA(A)=E_{SCA}$*(version number, serial number, validity period, A,* K_{PA}*, CA), CA* and *CA'* may be same or different.

For example (see **Figure 1**), mutual authentication for calling entity A and called entity B to setup a connection can be illustrated in **Figure 2**.

ATM networks, being large-scale and multi-organizational, will obviously need a multitude of CA's. The ATM nodes (i.e., endpoints or switches) in different organization domains will be certified by different certification authority entities. Therefore, it is necessary to specify CA included in the certificate during authenticating signalling messages in order to avoid confusion.

Because each of the security information elements which are inserted into signalling messages by our proposal is absolutely necessarily for mutual authentication of signalling message, the scheme is optimized and will provide rapid authentication of signalling message.

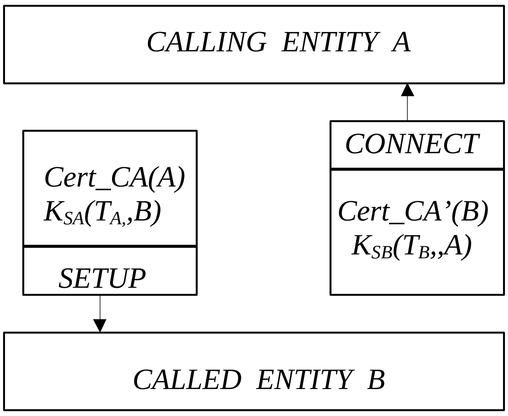

Figure 2. Example of mutual authentication for signalling message

2.2 Negotiation of Security Context

Only confidentiality and integrity services applied on user data may be negotiated. Based on differences between the methods for negotiating a security context, they can be divided into three sorts:

(1) negotiation through signalling information;
(2) negotiation through management information;
(3) negotiation through an auxiliary channel.

In our architecture, negotiating a security context begin after a connect between the node A and the node B has been set up. It is carried out by the user plane in ATM Protocol Reference Model. The procedure of negotiating a security context can be illustrated in the following figure.

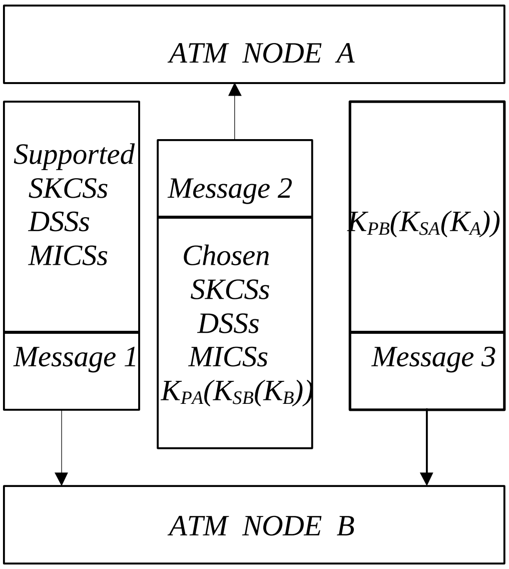

Figure 3 The procedure of negotiating a security context

In the above figure, *SKCS*, *DSS* and *MICS* respectively denote Secret Key CryptoSystem, Digital Signature Scheme and Message Integrity Checking Scheme. The Session key which is used to protect data stream between the node A and the node B is the joint of K_A and K_B..

As shown in **Figure 3**, our proposal for negotiating a security context is a three-pass protocol consists of three message as follows:

(1) Message 1: From the node A to the node B, providing a list of supported secret key cryptosystems, digital signature schemes and data integrity checking schemes.
(2) Message 2: From the node B to the node A, replying with a chosen secret key cryptosystem, a chosen digital signature scheme, a chosen message integrity checking scheme from the list provided by the node A and one half of session key.
(3) Message 3: From the node A to the node B again, providing another half of session key.

It is envisaged that our proposal for negotiating a security context also has mutual authentication property. In addition, if the private key of either A or B is compromised, the proposal is still secure. No assumptions are made about the session key length in our architecture, various user can comply with various countries regulation.

2.3 Exchange of User Data

Following negotiation of a security context, the data stream between the node A and the node B can be exchanged using the session key (K_A K_B) which was agreed during the negotiation of a security context.

According to distinctions between the methods for securing user data exchange, they can be divided into three sorts: (1) confidentiality at the higher layer; (2) confidentiality in the ATM layer; (3) confidentiality in the AAL layer.

Confidentiality in our proposal is placed at the high layer. The placement of security functions is shown in **Figure 4**.

The advantages of the solution for securing user data exchange lie in:

(1) It does not burden the ATM network with unnecessary functionality, where the main duty of ATM networks is to transfer data between endpoints.
(2) Security is arranged as per Virtual Channel (VC), which is most suited for ATM networks and complies with the ATM Forum *«Phase I Security Draft Specification»*.
(3) It provides a suitable solution for ATM attached LAN environment.

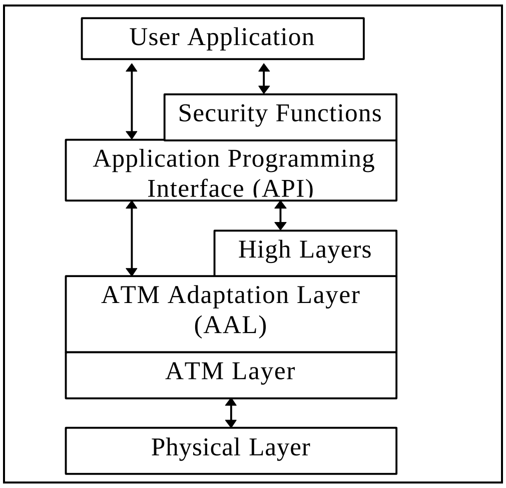

Figure 4 The placement of security functions

Due to the high volume data in ATM networks, any session key life time become very short. Thus, there is a requirement for mechanism to change the session key rapidly during the lifetime of a call. Our proposal for exchanging session key is inserting security synchronisation points into the data stream, which can initiate the change of session key and/or digital signature scheme.

3 Conclusion

A new proposal for securing communication over ATM networks is presented above. In the proposal, securing ATM communications can be divided into three following stages:

(1) rapidly authenticating signalling mess-ages (such as *SETUP* and *CONNECT*) by inserting optimized security information elements into them;

(2) negotiating a security context in the user plane;

(3) applying negotiated security services on the user data exchange.

Since sooner security specifications for ATM networks will be defined, simpler and more reliable the chosen security solution will be and wider the security services will be implemented within ATM facilities.

References:

[1] M. Peyravian, G.Tsudik and E.V. Herrewefhen, IBM, «A framework for authenticated key distribution in ATM networks», *ATM Forum/95-0580*.

[2] T. Smith, J. Stidd, Xerox Corporation, «Requirement and methodology for authenticated signalling», *ATM Forum /94-1213*.

[3] L. Pieson, T. Tarman, Sandia National Laboratories, «Requirement for security signalling», *ATM Forum/95-0137*.

[4] M. Lazer, Bellcore, «Framework for developing security-related signalling standards, *ATM Forum/95-0108*.

[5] S. C. Chuang, «Securing ATM networks», *Third ACM conference on computer and communication security*, New Delhi, India.

[6] R. H. Deng, L. Gong and A. A. Lazar, «Securing data transfer in asynchronous transfer mode networks», *Proceedings of Globecom'95*, pp. 1198-1202, Singapore.

[7] D. Stevenson, N. Hillery and G. Byrd, «Securing communications in ATM networks», *Communications of the ACM*, Vol.38, No.2.

[8] H. Cruickshank, Z. Sun and S. Velentzas, «A proposal for security services in ATM networks». *Fourth IFIP Workshop on Performance Modelling and Evaluation of ATM Networks*, Ilkley, July, 1996.

[9] M. Laurent, O. Paul and P.Rolin, «Securing communications over ATM networks», *Proceedings of IFIP SEC '97*, Copenhagen, Denmark.