A Lightweight Security Mechanism for ATM Networks

Ching-Yung Liu

Department of Information System, Chunghwa Telecom Co., Ltd. Central Taiwan Business Group, 8F, 161 Sec. 1, San-Ming Rd. Taichung, Taiwan 403, R.O.C. (Email: liucy@chtc.com.tw)

(Received March 25, 2005; revised and accepted April 22, 2005)

Abstract

The IP converge the multi-applications over Internet, and ATM will construct global networks for IP development. It is a significant research to associate those projects. The vision is that company or enterprise will have ATM switches on their own site to transfer bulk data across Internet. In this paper, we propose a lightweight security mechanism to support secure communications for ATM Networks. The mostly threats and attacks could be protected through authentication and confidentiality practiced in ATM networks. In our scheme, security parameter exchanges and session key generations are the engine that deployed under security module with in-band control. The security policy will process uncontrollable state with default criteria. We utilize an embed-policy as conflict resolution to promote the reliability of lightweight security system.

Keywords: Asynchronous transfer mode (ATM), authentication, confidentiality, cryptography, security policy

1 Introduction

ATM (Asynchronous Transfer Mode) techniques were developed on the B-ISDN standard about 20 years ago. The ATM has provided communication network operating and support functions with availability and reliability warranties. Beyond a doubt, IP is the multi-service convergence layer now and for the future. The next generation network infrastructure defines, evaluates, and implements an enhanced architecture for the QoS under IP Networks. ATM as the Internet platform to construct global networks will be a significant research area.

ATM switches possess many unique features in communication networks, such as, multi-service, individual QoS, connection-orientation and the ability to transmit through various physical media (SDH, SONET, F.R., etc.). The ATM Forum has enacted many standards that have been used in different network inter-connections. ATM multiplexing switches various services aggregated in high-speed trunks that float in the public network without shields. These services are insecure.

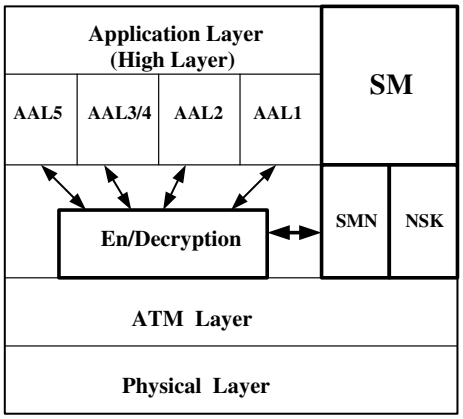

Figure 1: The placement of security functions

Although, ATM has many communication features, security is its' weakness. The users cannot pass sensitive or proprietary data through public networks because the public networks are open. We propose a lightweight security mechanism to provide security against the attacks and threats possible on open public networks. The basic network security defense is a lower layer gatekeeper on which a higher layer information system or equivalent will employ a secondary security protection layer. Many proposals have suggested establishing ATM security protection [2, 6, 10, 12, 13]. These inherent and intrusive mechanisms are mainly methodologies that produce secure shields in the user plane and control plane. Normally, point to point and point to multi-point systems are the entities usually protected. Public key algorithms matching symmetrical cryptographic systems are the most frequent applications.

In this paper, we propose a lightweight security mechanism for performing authentication and security to protect against the most likely threats and attacks. Our method (as Figure 1) supports end-to-end security applications combined with ATM inherent control capabili-

ties. AAL and AT-M layers are used to encrypt the user data while leaving the cell header in the clear [8]. The paper is organized as follows. In Section 2 we discuss some vulnerable situations in ATM communications and how to prevent attacks. In Section 3, we describe in detail the connection flow in lightweight ATM mechanisms. Section 4 analyzes the security parameter exchange and session key update protocol. The security policy that supports uncontrollable determination is discussed in Section 5. Section 6 presents our conclusions.

2 Security Threats and Prevents

As with most public networks, ATM networks are susceptible to several security threats and attacks [1, 11], as follows:

- Intrusions into the secrecy of communications.
- Forging tricks that present receivers with corrupted messages.
- Deceiving either the sender or receiver with a false identity.
- Denial of service attack.

2.1 Deceiving a User Using Masquerades

The SETUP is the initial signaling message used to establish an ATM switched virtual circuit (SVC) connection. The Setup IE (information elements) profiles include a calling party number, but that is an optional IE. The called party cannot be guaranteed to receive an authenticated calling party number in current ATM protocol reference model (PRM) designs.

In masquerading attacks, a hacker acts as an authorized user to gain privileges that could access information and resources. The ATM switches and end systems are identified by their ATM address that follows OSI NSAP (network service access point) standards. Usually the same group ATM end systems are connected to nodes using a common network prefix. Only different SEL (selector) values distinguish each end system. In the ATM system initial stage, the intruder could forge another SEL value for their active attacks.

As mentioned above, although calling party number is provided for verification, a masquerader's end system could dodge the ID check. We therefore propose an in-band authentication process that is launched after the path is established but before user data is sent. Since this authentication allows the sender and receiver to positively identify one another, a third party cannot impersonate either of the two. This extra authentication architecture enhances the ability for two parties to recognize one another based on the familiarity between these individuals.

2.2 Secure Communications Intrusions

A hacker intercepts a connection for eavesdropping or fabrication. This frequently happens in a public network and allows attacks against valuable data during transmission. Effective confidential algorithms could protect against these threats. In a secure environment, attacks by hackers will be prevented and easily discovered. Generally, the end user will adapt sensitive data to a MAC (message authentication code) format that attaches to the message to achieve data integrity. Denial of service and interruption attack belongs to the destructive class of attacks. In ATM signaling, messages [4] such as, Setup, Restart, and Clear used to construct or reallocate resources associated with the virtual circuit identification (VCI) could be used to form traffic floods to paralyze a designated user service. To prevent these kinds of attacks, additional mechanisms are needed. Measures such as guards against unauthorized physical access, fault locking mechanisms and limited retry allocations, etc. can be instituted. In this paper, we will not consider these types of attacks for such a lightweight security system.

3 Secure Services and Control Schemes

The system in our architecture utilizes the sequence depicted in Figure 2. We create a security module (SM) and use a symmetrical key algorithm, such as DES (data encryption standard) to accomplish the encryption operations. There are several cryptographic products [5] available to encrypt data traffic under 155Mb/s with DES operational modes. The necessary procedures are embedded into the security end systems. Signals or messages can then be passed transparently along the connection path. The SM selectively switches between the active mode or doze mode and maintains only a transient secure control process within a session. The SM is a software module that resides as a daemon.

A shared key algorithm, like a DES-CBC (DES-cipher block chaining) mode executes the data security. This is a default element for confidential data applications. Our scheme allows other algorithms through negotiation. The public key algorithm distributes the keys using a digital envelope. Our mechanism pre-places the public key into a partner end system. The certification authority (CA) will be accessible if optional certificate verification is used. The detailing description of connection flow is explained in the following two subsections.

3.1 Security Service Preparation

The ATM signaling protocol designates the message sequence for establishing or releasing connections. The reference configurations and flow are illustrated in Figure 2. SM is the principal component for coordinating the specific flow between the ATM signaling protocols. During

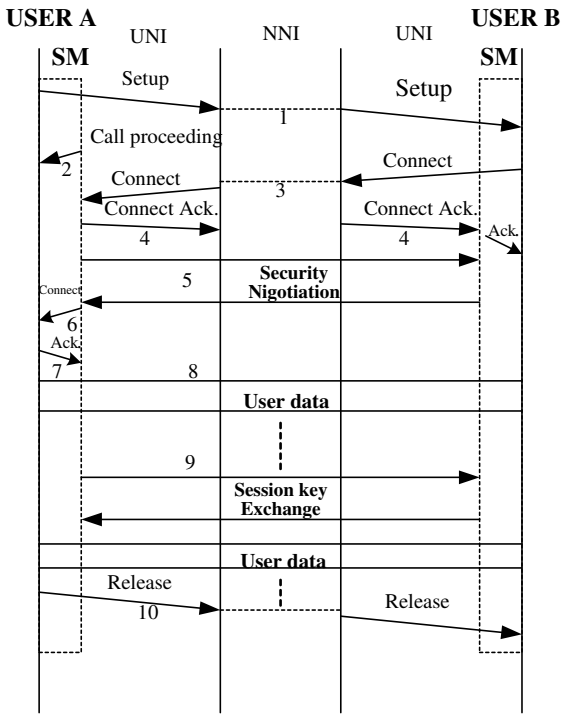

Figure 2: The control flow of ATM connection

the preparation stage, the SM acts as a security controller to confirm service between two peers. The steps are as follows:

Step 1: For requesting a connection to carry user information, the SETUP message includes the class type, traffic description, called party number and required QoS etc. The ATM switches rely on the IEs to determine the destination node allocation to accommodate the called party. The IEs for the called party number has a 25 bytes length to accommodate the 20 bytes ATM NSAP address. A byte message was added into the called party IE number to initialize the remote SM. This message consists of a 4-bit Version and 4-bit SubID field to activate the called user SM functions.

Step 2: The setup request will enable a counter to monitor the response time. If the SETUP fails to respond within the time limit (4 seconds), then the calling party initiative sends the SETUP message again. The CALL PROCEDURE can extend the time limit to 10 seconds. The SM can activate the call procedure message to end the process, if necessary.

Step 3: The CONNECT signal indicates call acceptance by the called user. This message is sent by the called user to the network or by the network to the calling user. Upon receipt of a CONNECT message from the called, the SM prohibits a CONNECT message sent to the calling user.

Step 4: The SM holds the CONNECT message and sends a CONNECT ACK to respond to the ATM switches. Simultaneously, the called party will receive a CONNECT ACK message.

3.2 In-band Negotiation for Security Services

When a connection has been established, the lightweight system enforces negotiation and exchange parameters on the path. The SM will produce a secret communication link and monitor the session until the connection is released.

Step 5: After the VPC/VCC is settled, the calling party's SM activates the security parameters to the called SM. A session key is randomly created, authenticated, and exchanged with the peer SM. The called party responds under proper authority and within the time limit. If the authentication process fails, the calling SM, on the basis of the security policies, will decide whether to release the link. The detailed description of the security message negotiation (SMN) will be presented in the next section. If the calling party sends the SMN twice and no SMN responds, the remote party cancels the link without the SM functions.

Step 6: Upon successful completion of the security negotiation, the subsequent user data transmitted would be protected. The SM releases the ban and conveys the previous CONNECT messages to the calling system.

Step 7: The calling systems respond CONNECT ACK to start the data transmission. Simultaneously, the called party's SM also unblocks the user data.

Step 8: If the user data accord SMN negotiation for private communications utilizes confidential encryption. The SM can be switched to the doze mode during this period.

Step 9: If a long-term connection is required, the session key can be refreshed using a new key operation that can be initialized by either party. We propose an in-bind key update operation embedded in the security module to provide simplicity and a transparency advantage. Disrupted service to the user is the weakness in this system. The detailed description of the key lifetime will be presented in the next section.

Step 10: The communication path is invoked in the user's initializing operation. The RELEASE message to unload the resources allocated for the connection is then sent. The SM then switches to the doze mode again.

4 Secure Messages Negotiation and Session Key Generation

We proposed both security message negotiation and new session key (NSK) protocols. These protocols are in-band controlled to implement a novel and flexible mechanism.

4.1 Secure Messages Negotiation (SMN)

As shown in Figure 3, the calling party assumes the initiating role and the called party assumes the response role, with notations and operations as follows:

- ks: Session key, the first session key is shared for data confidentiality. The same ks are offered in a bi-direction connection that simplifies key management by reducing the load and improving performance.
- N_x: Nonce, a random generated number that provides both legal authorization and prevents the replay attack.
- ID_x: Identities of the two communicating parties. The ATM address or unique assignment code would be used.
- $Conf-Opt$: Confidential option, provides two symmetrical algorithms; the initiator according his assigned accessibility and an optional selection or dedicated operation (default element).
- IV: The initial vector for symmetrical algorithms (like, DES-CBC).
- $(\cdot)_{pk_x}$: Encrypts the message using a public key X.
- $(Cert_x)$: Certification from certificate authority (CA) offered for key authentication in a public key system.
- $(Hash(\cdot))_{sk_x}$: The hashed result when the message is signed using the private key of X. The hash is assumed to be a one-way hash function, such as the message digest 5 (MD5) [3] or secure hash standard. Hash function announced to public.

User A sends an initial SMN to user B.

The first session key, Nonce and ID_a is pre-selected during the SMN preparation which is associated with $Conf-Opt$ and the initial vector (IV) to form a token to be encrypted using B's public key. $Cert_a$ is an optional token to check the validity of A's public key. The one-way hash function enforces the message integrity and allows B to authenticate user A.

- User B response SMN to user A

When B receives the initial SMN. He Decrypts the cipher with his corresponding private key and checks its validity. The called party performs a hash operation to produce a reply to the message integrity checks. If A is not a proper authority party then B discards the negotiation. If A's $Conf-Opt$ is optional then B could make a selection or the default confidentiality algorithm is settled.

When A received B's SMN, the parameter is extracted and interpreted. A then Checks if the received N_a that is identical to A's first SMN.

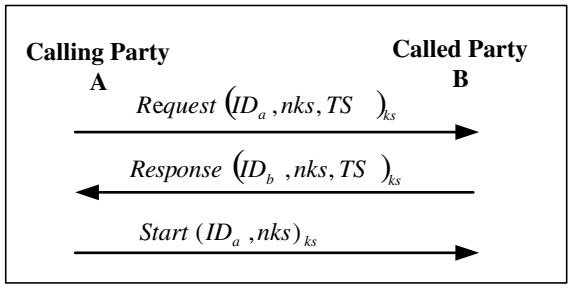

Figure 4: Session key modification protocol

4.2 Session Key Generation

A session key update is one of the crucial issues to guarantee the security of communications. A longer session key lifetime will increase the probability of attack. The ATM Forum technical committee proposal uses OAM (operation and maintenance) cell, such as, F4, F5 OAM to update end-to-end VPC (virtual path connection) and VCC (virtual channel connection) session key. OAM is defined in the management plane, if this scheme is used a more complex security system will be required that will disturb the transparency properties. In our lightweight security mechanism, we propose a novel in-band session key update that will periodically update the session key. The session key update is determined by the security policy. The key update flow is shown in Figure 4.

- New session key distribution:
  The initiator creates a new sessions key (NSK) and invokes a request message for updating the session key. Both the calling or called party could to be the initiator. The TS (time stamp) is attached to prevent the replay attack. These two parameters are encrypted using the session key (ks).
- Response NSK:
  When B receives the NSK, the cipher is decrypted with the corresponding session key and its validity checked. If the TS is received within a reasonable time, B responds with an NSK to the calling party and stores the new session key. If the TS fails in check or A is not a proper authority, then B ignores the request.
- The Initiator sends the NSK:
  After sending the NSK, the initiator waits for a response. If the specified delay time is reached, the request will be resent (maximum twice). If the NSK response is received, a check will be made and the results will determine whether another NSK is resent.

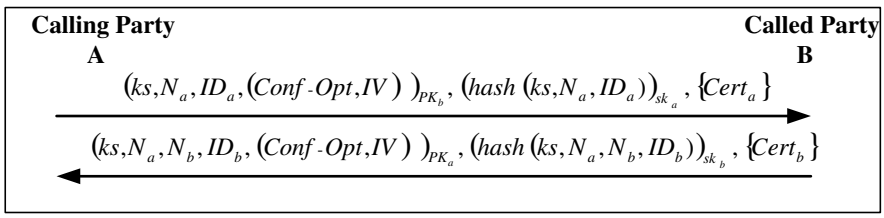

Figure 3: Session key negotiation protocol

Using the NSK is an obligation for the initiator. A start NSK message is sent 3 times to guarantee receipt. The time interval for the start token is set at one second. Once the session key update is complete, the SM de-activates into the doze mode.

5 User Security Policies

More than one policy could be embedded into this lightweight security ATM system. Our security service schemes have neither signaling control nor OAM control [7], but use simplified in-band control methods. Since, we need additional policies to determine conflict resolution and to maintain the synchronization with the security partner, different individual policies can negotiate the same solutions. Additionally, some errors could depend on the settled policy. In our in-band security system, the session key negotiation and modification can been approached by any parties at any time. With this feature the security system can establish re-negotiations for severe errors unless that action has already reach its' limitation. The different policies invoke distinct processes. Normally, almost every connection would operate with the A and C (authentication and confidentiality) security level in the same group. But with some ordinary connections, we could lower the security level or without security mechanism according security policy. If different groups of users operate on different security levels that will be deemed based on the highest policy criteria, another application would determine the new key or discard the connection. Policies could be consolidated among enterprises or groups.

Our in-band mechanisms provide control regardless of the product version with easy end terminal development. In-band control will disrupt the user data stream and require a watchdog program to detect the events for the session key exchange. In SMN negotiation we prohibit the CONNECT message and could activate a Call Proceeding message that provides sufficient time without interrupting the data stream. To change keys, rapidly and simply is our goal for this lightweight system. During NSK, the Initiator need only insert a Request message then keep the user data transmitting the Response message sent as request message that would not affect the user's communication. We also designed a trigger signal embedded in the NSK cell that gives a sign to the watching-dog program to invoke the NSK procedure.

Although the ATM Forum Specification 1.0 [9] provides security services between point-to-point or point-to-multipoint, even a multiple associations with nesting could reside in the security agent in ATM switches. The problems are how to upgrade an existent ATM network and whether the manufacturers are willing to implement those functions into their new products? What are the benefits for the end users with complexity mechanisms? How many users need these functions? In fact, that depends on the user demands. Customer-orientation is the key point for ATM security services development. Widespread security mechanisms will be deployed in the future.

6 Conclusions

We proposed a lightweight security mechanism for ATM end systems that considers the demand-oriented trend. Our mechanism provides instant ports to existent user end systems. This lightweight system would already satisfy most of end users for their security requirements. Moreover, today encrypt-speed techniques limit the encryption speed under 155 Mb/s, the speed suitable for end systems to implement security crypto-systems. Although parallel encryption devices may acquire more high-speed output, the complexity control and synchronization recovery will create extra problems.

In lightweight security systems, the cryptographic key agility and error extension invoked from cell loss are easy to overcome. We proposed in-band security negotiation and key update schemes that allow both permanent virtual connection (PVC) and SVC to fulfill the security environment. The majority of existent ATM networks barely support PVC. Those PVC connections could also perform negotiation and session key update with our mechanism. Due to the lightweight design, we used policies to handle some uncontrollable conditions to synchronize our protocol. Even in severe error situations the RESTART message can rebuild the connection. As in most of public key algorithm problems, if the user wants to verify the certification, convenient CA deployment will be reachable by the end systems. Our security mechanism provides both parties with a safe environment that efficiently guards to against eavesdropping, traffic tampering and masquerades, which establishes ensured secrecy on

public network communications.

References

[1] S. C. Chuang, "Securing ATM networks," in *Proceedings of The ACM Conference on Computer and Communication Security*, pp. 19–30, 1996.

[2] Z. Fan, "New trends in ATM networks: A research view," *Computer Communications*, vol. 22, no. 6, pp. 499–515, 1999.

[3] IETF. "The MD5 message digest algorithm,". Tech. Rep. 1, RFC 1321, April 1992.

[4] ITU-T. "B-ISDN application protocols for access signaling WTSC resolution,". Tech. Rep. 1, ITU-T Recommendation Q.2931, Feb. 1995.

[5] S. Kuhn, C. Ruland, and K. Wollenweber, "ATM-encryption with 155 Mbit/s," in *ATM Workshop, 1999. IEEE Proceedings*, pp. 307–312, 1999.

[6] M. Laurent, "Secure communications in ATM networks," in *IEEE 15th Annual Computer Security Applications Conference*, pp. 84 –93, 1999.

[7] M. Peyravian and T. D. Tarman, "Asynchronous transfer mode security," *IEEE Network*, vol. 11, no. 3, pp. 34–40, 1997.

[8] D. Stevenson, N. Hillery, and G. Byrd, "Secure communications in ATM networks," *Communications of ACM*, vol. 38, pp. 45–52, Feb. 1995.

[9] The ATM Forum Technical Committee. "ATM security specification, version 1.0,". Tech. Rep. AF-SEC-0100.000, The ATM Forum Technical Committee, Feb. 1999.

[10] V. Varadharajan, R. Shankaran, and M. Hitchens, "On the design of secure ATM networks," *Computer Communications*, vol. 22, no. 15, pp. 1512–1525, 1999.

[11] V. Varadharajan, Rajan Shankaran, and Michael Hitchens, "Security services and public key infrastructure for ATM networks," in *22nd Annual Conference on Local Computer Networks*, pp. 253–262, 1997.

[12] David O. Williams, "A review of wide-area aspects of high performance networking," *Simulation Practice and Theory*, vol. 6, no. 2, pp. 99–118, 1998.

[13] X. Yi, K. Y. Lam, and Y. Gong, "A proposal for securing communications over ATM networks," in *IEEE International Conference on Information, Communications and Signal Processing*, pp. 631 – 634, Singapore, 1997.

Ching-Yung Liu was born on October 10, 1958 in Taichung, Taiwan, Republic of China (ROC). He received the B.S. in electronic engineering from National Chin-Yi institute of technology, Taichung, Taiwan, ROC, in 1985 and the M.S. degree in Information Management in 2001 from Chaoyang University of Technology, Taichung, Taiwan, ROC. He is working in Chunghwa Telecom Co., Ltd. at Planning/designing and information Department. He majors in telecommunication of transmission. His research interests include: commu- nications (ATM) security, cryptography, IP security and broadband networks security.