ATM 보안 취약성 분석

강상구, 이성우, 신재호
동국대학교 전자공학과

Analysis of ATM Security vulnerability

Sanggoo Kang, Sungwoo Lee, Jaeho Shin
Dept. of Electronic Eng., Dongguk University
E-mail : sgkang@cakra.dongguk.ac.kr

Abstract

In recent years, security has been more and more significant in network environment. The internetworking communication including ATM network will be exposed to all kinds of attacks, such as eavesdropping, spoofing, service denial and traffic analysis etc. So, in this paper, we focused on ATM network threats, security service and ATM security mechanisms for threats.

1. 서론

최근, 인터넷의 출현과 함께 네트워크 환경에서의 보안이 더욱더 중요시되고 있다. 보안 기법을 함께 제공하지 않는 대부분의 네트워크 기술은 몇몇 보안 서비스를 제공하기 위해 다시 설계되어야 하는데 ATM(Asynchronous Transfer Mode)도 이러한 기술들중 하나이다.

향후 멀티미디어 서비스를 처리할 초고속 정보 통신망(B-ISDN) 기술을 구현하기 위해 음성, 영상, 데이터 전부를 하나의 네트워크로 보내는 멀티미디어 통신 네트워크를 구현하는 기술의 핵심인 비동기 전송모드 ATM이 출현하게 되었고 또한 ATM은 B-ISDN에만 제한되지 않고 다양한 네트워크 연결을 위해 간단하게 네트워크 기반(LAN, MAN 또는 WAN) 제공을 위해 이용될 수 있다. 그러나 다른 네트워크와 마찬가지로, ATM 망도 도청(Eavesdropping), 스푸핑(spoofing), 서비스 거부, 트래픽 분석(traffic analysis)과 같은 많은 위협요소들이 있음에도 불구하고 현재로서는 보안 서비스를 제공하지 않는다는 것이 취약점으로 남아있다.[1][2][3][4][5][6] 이러한 위협요소들을 방어하기 위하여 정보 보호 기능을 ATM 시스템에서 어디에 적용하고 어떻게 적용할 것인가 하는 점이 대두되고 있으며 현재 ATM Forum에서 진행 중에 있다.

본 논문의 2장 ATM의 개요에서는 ATM 시스템의 정보 보호를 위한 방안을 연구하기 위해 필요한 ATM의 기본구조와 기능 등에 관하여 설명하고, 3장에서는 ATM 망의 위협요소 그리고 4장에서 ATM 보안 서비스인 데이터의 무결성과 기밀성, 송수신단간의 인증, 그리고 접근제어에 대해 설명한다. 5장에서는 4장에서 언급한 보안 서비스를 제공하는 보안 메카니즘에 대해 설명하고 6장에서 결론을 맺는다.

2. ATM의 개요

ATM은 회선교환과 패킷교환 양쪽의 장점을 갖춘 아키텍처로서 53바이트의 짧은 셀 길이의 데이터 단위로 메가비트에서 기가비트까지의 전송속도에 유연히 대응할 수 있을 뿐 아니라 교환처리의 대부분을 하드웨어로 행하기 때문에 멀티미디어 통신을 위한 저 지연, 고속 네트워크를 할 수 있다.

2.1절에서 ATM의 셀 송·수신 과정에 대해 간략하게 설명하고 2.2, 2.3, 2.4절에서 그림 1. ATM 프로토콜 참조 모델의 구조에 대해 설명한다.

2.1. ATM 셀 송·수신 과정

ATM에서는 양단이 통신하려할 때 먼저 교환기로부터 가상 채널을 받아 연결이 성립된 후 데이터를 전송한다. 비록 양단은 데이터의 크기에 상관없이 보낼 수 있지만 ATM 적응 계층에서 송신측의 단말에서 수신측의 단말로 보내는 정보를 48바이트씩 나누고, ATM 계층에서는 수신처 레이블 정보인 5바이트의 헤더를 덧붙여 53바이트의 고정길이를 가진 셀이라고 하는 단위로 정보를 송신한다. ATM 네트워크 내로 보내진 셀은 수신처 레이블 정보에 따라 하드웨어에 의해 고속으로 교환된다. 그래서, 수신측의 단말에 도착한 셀

은 레이블 검사를 받고 원래 정보로 재구성된다. 이와 같이 ATM은 같은 수신처 레이블 정보를 가진 셀의 송신개수를 변화시킴으로써 통신 채널의 대역용량을 시간적으로 바꿀 수 있어 통신 속도에 의존하지 않는 네트워크가 실현될 수 있다.

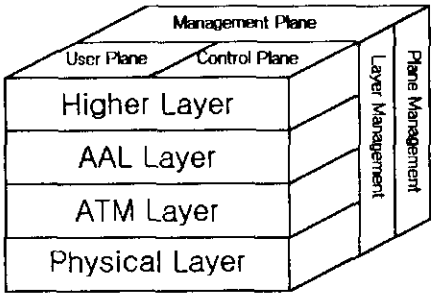

그림 1. ATM protocol reference model

2.2. ATM 계층

53바이트의 셀을 처리하는 계층으로 48바이트의 사용자 데이터와 5바이트의 헤더로 구성된다. 헤더에는 각 단말에서 발생하는 트래픽의 흐름을 제어하기 위한 일반적인 흐름 제어(Generic Flow Control, GFC) 가상 채널을 식별하는 가상 채널 식별자(Virtual Channel Identifier, VCI)와 가상 패스를 식별하는 가상 패스 식별자(Virtual Path Identifier, VPI), 페이로드(사용자 데이터) 유형을 식별하는 페이로드 타입(Payload Type, PT), 폭주상태에 빠졌을 때 중요하지 않은 셀부터 먼저 폐기하기 위한 셀 손실 우선표시(Cell Loss Priority, CLP), ATM 셀 동기를 위한 헤더 오류제어(Header Error Check, HEC)로 구성된다[7].

2.3. AAL 계층(ATM Adaptation Layer)

여러 가지 상위 애플리케이션의 데이터 단위(수 킬로 바이트까지의 가변길이)를 셀의 48 바이트 사용자 정보와의 정합·조정을 행하는 계층으로 수렴 부계층(Convergence Sublayer)과 분리 및 재결합 부계층(Segmentation and Reassembly Sublayer)으로 구성된다[8].

2.4. Plane 구성

사용자 데이터를 전송하는 User plane, 상대 단말과의 호 설정과 해지에 관련된 제어 정보를 처리하는 Control plane 그리고, User plane과 Control plane에 관련된 관리정보를 처리하는 Management plane으로 구성된다.

3. ATM 망의 위협요소

이 장에서는 ATM망에서 도출되고 있는 위협요소들을 살펴보고 이러한 위협요소에 대응하는 보안 서비스를 4장에서 기술하겠다.

- 도청(Eavesdropping)

  네트워크에서 가장 일반적인 공격중 하나로 전송매체를 도청하여 데이터에 대한 비합법적인 접근을 얻어내는 것을 말한다. ATM은 광케이블로 연결되어 있기 때문에 다소 어려움이 있으나 약 $2,000정도의 광케이블 도청장치만 있으면 도청이 가능하다[9].

- 스푸핑(Spoofing)

  단순히 정보를 얻기 위해 또는 파괴할 목적으로 리소스에 접근하기 위해 다른 사용자로 위장하는 것을 말한다. ATM 네트워크 또한 인터넷을 통해 많은 인가되지 않은 네트워크와 연결되기 때문에 해커에 의한 공격으로부터 보호할 수 없다.

- 서비스 거부(Service Denial)

  ATM에서의 연결은 SETUP 신호에 의해 성립되고 RELEASE 또는 DROP PARTY 신호에 의해 단절된다. 만약 해커가 RELEASE 또는 DROP PARTY 신호를 특정 교환기에 빈번히 보내게 되면 사용자간의 통신은 방해되고, 이로인해 ATM의 QoS(Quality of Service)를 손상시킬 수 있다[10].

- 트래픽 분석(Traffic analysis)

  ATM 셀의 페이로드 부분은 암호할 수 있는 반면, 헤더 정보는 암호화 될 수 없기 때문에 해커는 셀의 헤더 정보와 라우팅 테이블의 정보를 얻어 사용자 데이터가 어느 시간대에 어떠한 량을 가지고 송신되고 있는지를 알 수 있고, 이러한 정보를 가지고 채널을 변환시킬 수 있다.[6]

4. ATM 보안 서비스

이 장에서는 3장에서 언급한 보안 위협요소에 대응하기 위한 보안 서비스를 기술한다. ATM 포럼에서는 현재, 사용자 플래인(User Plane)과 제어 플래인(Control Plane), 관리 플래인(Management Plane) 보안 서비스로 나누어 언급하는데 제어 플래인과 관리 플래인은 현재 계속 진행중에 있다[11][12].

4.1. 일반적인 네트워크 보안에서의 요구 사항

- 인증(Authentication)
  자신이 특정한 상대에게 보낸 정보가 자신이 의도한 상대방에게 올바로 전달되어야 한다.
- 기밀성(Confidentiality)
  인가 받은 사용자만이 데이터에 접근할 수 있다.
- 무결성(Integrity)
  전송되는 데이터가 제 3자에 의해 변경될 수 없다.
- 부인봉쇄(Non-repudiation)
  사용자가 데이터에 접근한 사실을 부인할 수 없다.

4.2. ATM 포럼에서 언급한 보안 서비스

- 사용자 플래인(User Plane) 보안 서비스
  전송되는 사용자 정보를 보호하기 위해 제공
  - 접근제어(Access Control)
    인가된 사용자만이 리소스에 대한 접근권한을 갖도록 하기위한 보안 서비스
  - 인증(Authentication)
    전송되는 사용자 정보가 타당한 수신자에게 수신되도록 하기 위해 양단의 신분을 상호 확인하는 절차가 필요하며, 키 교환과 같은 다른 보안 서비스에 이용될 수 있다.
  - 데이터 기밀성(Data Confidentiality)
    도청(eavesdropping)과 같은 공격에 대응하기 위한 서비스로 적합한 키를 소유하고 있는 수신자만이 복호화 할 수 있도록 ATM 셀의 48바이트 페이로드 부분을 암호화한다. 5바이트의 헤더 부분은 암호화 되지 않는다.
  - 데이터 무결성(Data Integrity)
    데이터의 원본을 인증하는 것으로 사용자 정보 자체를 변경시키는 것에 대응할 수 있다.
- 제어 플래인(Control Plane) 보안 서비스
  상대 단말과의 호 설정과 해지에 관련된 제어 정보를 보호하기 위해 제공
  - 인증(Authentication)
    스푸핑(spoofing)과 같은 공격에 대응하기 위한 서비스이며 출처가 분명하지 않은 메시지는 무시하기 때문에 서비스 거부(Service Denial)에도 강력히 보호될 수 있다.
- 보안 메시지 교환 프로토콜과 기본적인 협상(negotiation)
- 제어 플래인(Control Plane)에서의 안전한 메시징
- 키 교환
- 세션키 갱신(update)
- 인증서 기반(certificate infrastructure)

또한 ATM 포럼에서는 보안 서비스들에 사용할 파라미터를 협상(negotiation) 하거나 엔터티 인증 서비스를 제공하기 위해 2가지 방법의 보안 메시지 교환 프로토콜을 정의하고 있다. 첫 번째, 3 단계 보안 메시지 교환 프로토콜(3-way security message exchange protocol)은 보안 옵션의 협상을 요구하는 연결에 사용되고, 이 프로토콜은 동기화를 위한 타임 스탬프를 사용하지 않는 장점이 있다. 두 번째 방법으로 2 단계 보안 메시지 교환 프로토콜(2-way security message exchange protocol)이 있는데 이 프로토콜은 보안 파라미터 협상이 필요하지 않는 연결에 사용된다. 이 프로토콜은 보안 정보를 생성하거나 확인하기 위해 송수신단간에 시간 동기화가 요구된다.

3 단계 보안 메시지 교환 프로토콜은 아래의 그림 2와 같은 단계를 거치며 수행하게 된다.

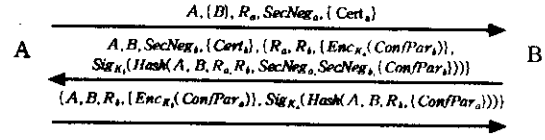

그림 2. 3 단계보안 메시지 교환 프로토콜

2 단계 보안 메시지 교환 프로토콜은 아래의 그림 3과 같은 단계를 거치며 수행하게 된다.

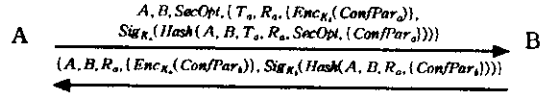

그림 3. 2 단계보안 메시지 교환 프로토콜

위 그림들에서 사용되는 용어는 표 1과 같다.

ATM망에서 안전하게 통신을 하기 위한 보안 메커니즘은 일반적으로 3 단계의 과정을 수행한다[13]
1단계는 시그널링(signalling) 메시지의 인증,
2단계는 보안 메시지의 협상(negotiation),
3단계는 사용자 데이터의 교환 등을 거친다.

5. ATM 보안 메커니즘

이 장에서는 4장에서 언급한 보안 서비스들을 지원할 수 있는 보안 메커니즘을 기술한다. ATM 포럼에서 기술한 보안 메커니즘은 아래와 같은 보안 서비스들을 지원하고 있다[11].

X	엔터티 X의 식별 이름
K_X	X가 사용하는 키
$Enc_{K_X}(text)$	X의 키로 text를 암호화
$Sig_{K_X}(Hash(text))$	X의 키로 text를 해쉬한 것에 전자 서명
$Hash(text)$	text의 일방향 해쉬
R_X	X에 의해 생성된 난수
T_X	X에 의해 생성된 타임 스탬프
{,}	옵션토큰
SecOpt	2 단계 보안 메시지 교환 프로토콜에서, 송신자가 수신자에게 통신에 사용할 보안 서비스를 알려주는데 사용
*SecNeg_*	2 단계 보안 메시지 교환 프로토콜에서, 송신자와 수신자가 통신에 사용할 보안 서비스 또는 파라미터를 협상하는데 사용
*ConfPar_*	송신자로부터 송신자 키를 비밀리 수신자에게 전달하기 위해 사용
*Cert_*	3 단계 보안 메시지 교환 프로토콜에서, 송신자나 수신자가 상대방에게 인증서를 제공하기 위해 사용

표 1. 프로토콜에 사용되는 용어

시그널링 메시지 인증 관계에서는 송수신단간의 인증을 수행하는 단계이고 보안 메시지 협상단계에서는 송수신단간의 사용할 보안 서비스를 협상하는 단계이다. 그리고 마지막으로 사용자 데이터 교환 단계에서는 보안 메시지 협상 단계에서 서로 동의한 키를 사용하여 데이터를 주고받는다.

6. 결론

향후 멀티미디어 서비스를 빠르고 원활하게 제공하기 위해 ATM 망의 이용은 급증하게 될 것이다. 이에 본 논문은 ATM의 많은 장점에 비해 보안상의 많은 취약성을 가지고 있음을 보안 위협요소를 연급하면서 살펴보았다. 또한 이러한 보안 위협요소들을 방지하고 대처하기 위한 보안 서비스들과 이를 지원하기 위한 일반적인 보안 메커니즘에 대해서도 살펴보았다. ATM의 보안에 대해 몇 년 전부터 세계 여러 곳에서 많은 연구와 논의가 진행되어 오고 있다. 이러한 추세에 발맞추어 우리 나라에서도 ATM 보안에 대한 많은 관심과 연구가 진행되어야 할 것이다. 그리고 또한 ATM 보안에 이용할 수 있는 국내 암호 기술 및 보안 기술에 대한 연구가 필요할 것이다.

참고문헌

[1] Maryline Laurent, Olivier Paul, Pierre Rolin, "Securing communications over ATM networks", IFIPSEC'97, Copenhagen, Denmark, May 1997

[2] L. Hanson, "The Impact of ATM on Security in Data Network", Proc. of Compsec International 1995, Conf. 12, pp 318-324

[3] Shaw-Cheng Chuang, "Securing {ATM} Networks", 3rd {ACM} Conference on Computer and Communications Security, New Delhi, India, 1996, pp.19-30

[4] R. Deng et al, "Securing Data Transfer in Asynchronous Transfer Mode Networks"; Proceedings of GLOBECOM'95, Singapore, November 13-17, 1995, pp. 1198-1202

[5] J. Kimmins and B. Booth: "Security for ATM networks"; Computer Security Journal; XII(1):21-29; 1996

[6] Richard Taylor, Greg Findlow, Asynchronous Transfer Mode: Security Issues, Proc. Australian Telecommunication Networks and Applications Conference;pp. 161-166, 5-7 Dec. 1995; pp. 161-166

[7] B-ISDN ATM Layer Specification, ITU-TSS Recommendation I.461, June 1992

[8] B-ISDN ATM Adaptation Layer(AAL) Specification, ITU-TSS Recommendation I.363 (Proposed Revision)

[9] M. Bacon, Security: a question of confidence, Telecommunications (int. ed.) (USA) Vol. 23, No. 11, pp 51-52, Nov. 1989

[10] D. Stevenson and N. Hillery and G. Byrd, Secure communications in {ATM} networks Communications of the ACM, Volume 38, No 2, pp 45--52, Feb, 1995

[11] Security Working Group, Phase I ATM Security Specification, ATM Forum BTD-SEC-01.03, July 1997

[12] Mohammad Peyravian and Thomas D. Tarman, "Asynchronous Transfer Mode Security", IEEE Network, June 1997

[13] X. Yi, K.Y.Lam, Y.F.Han and Y.Gong, "A Proposal for Securing Communications over ATM Newworks", IEEE, 1997