主題

ATM Network Security 기술과 데이터 보호 방법

한국외국어대학교 한 치 문
한국정보보호센터 김기현, 김홍근

차 례

I. 서 론

최근 인터넷은 새로운 멀티미디어 응용 서비스 개발에 힘입어 음성 및 영상과 같은 스트림형(stream type) 서비스를 수용하는 방향으로 전개되고 있다. 이러한 추세에 발맞추어 네트워크 하부 구조도 고속화 되어가고 있다. 특히 인터넷 또는 초고속통신망의 하부 네트워크는 ATM 망을 기반으로 하여 진행되고 있다. ATM 네트워크는 음성, 데이터, 비디오 등의 서비스를 통합하여 전달 교환하는 멀티미디어 네트워크이다. 그러나 초창기 ATM 서비스는 데이터 서비스를 중심으로 한 인트라넷 구축에 초점을 맞추고 있다.

ATM 네트워크는 기본적으로 커넥션 기반 통신을 하는 구조인 반면에 기존의 데이터는 비연결형 통신 방식을 취하고 있다. 그러므로 ATM 네트워크에서 비연결형 데이터를 효율적으로 제공하는 방법이 여러 곳에서 검토되고 있다. 대표적인 방법으로는 CIP(Classical IP), LANE, MPOA 등이다. 이러한 방식 검토에 이어 IP 교환을 Cut-through 형태로 취급하는 IP Switching 방식에 대한 검토가 진행되고 있으며, ATM 네트워크에서 IP 통신을 위한 유력한 방식중의 하나로 위치를 확고히 하고 있다. 이처럼 ATM 네트워크 기반의 초고속통신망을 구축하고, 초고속통신망에서 다양한 구성원이 갖는 기업 네트워크를 구축하여 부가가치가 높은 다양한 서비스를 신뢰성 있고 안전하게 제공하는 것은 필수 불가결한 사항이다.

그러나 ATM 네트워크를 이용한 멀티미디어 통신에서는 가입자 액세스 라인을 여러 가입자가 공유하여 사용하고 있다. 한 가입자 선로에서 이론적으로 2^{24}개의 가입자가 접속될 수 있으며, VPI/VCI

값에 의해 가입자를 식별한다. 실제 시스템에서는 한 선로에 4,096개의 가입자가 접속할 수 있도록 설계하고 있다. 즉 매체 공유형의 액세스 형태로 구성되며, 고속 버스트성의 트래픽이 주류를 이루고 있다.

이처럼 한 개의 가입자 회선을 다양한 사용자가 공유하는 ATM 네트워크를 통해 특정 구성원(그룹) 별로 전용 네트워크를 구축할 필요가 있다. 이러한 형태의 네트워크가 더욱 경제적이라는 사실은 누구도 부정할 수 없다. 즉 ATM 네트워크를 인프라로 하는 VPN(Virtual Private Network) 구축이다. 오늘날 하부 네트워크는 ATM 네트워크로 하고 ATM 네트워크에서 논리적으로 서로 다른 VPN를 구축하여 정보 전달을 시도하고 있다. 동일한 인프라에서 서로 다른 VPN이 공존함으로 VPN간의 정보 누설 또는 도청의 위협이 전용망보다 강하게 느껴진다. ATM 네트워크를 인프라로 하여 정보전달을 초고속으로 실현하였으나 데이터를 안전하게 목적지까지 전달할 수 있는 방법에는 한계가 있다.

ATM 네트워크에서 보안의 중요성이 인식되어 ATM Forum를 중심으로 ATM 데이터 전달에 대한 보안의 표준화가 이루어지고 있다. 그 결과 1998년 12월에 ATM Security Version 1.0이 완성되었으나, 실제 적용에는 구체화 되어야 할 사항이 많다. 따라서 ATM 네트워크에 보안 기술을 적용할 때, 우선 고려하여야 할 점은 ATM 네트워크 프로토콜 모델을 변경하지 않고 구현할 수 있는 보안 모델과 최소한의 비용(Overhead)으로 Security Performance를 유지할 수 있는 보안 모델이어야 한다.

본 고에서는 ATM 네트워크 보안 기술에 대한 요구 사항과 ATM 네트워크에서 보안의 취약성을 분석하고, ATM Forum을 중심으로 한 ATM 보안 모델을 소개하고, ATM-WAN 환경에서 전달되는 데이터를 가입자 유형별로 나누고, 데이터 보호를 위한 한 방법을 설명한다. 그리고 금후 ATM 네트워크에서 전개될 네트워크 보안의 주요 내용을 간략히 요약 정리한다.

2. ATM 네트워크 보안 요구 사항

ATM 네트워크를 통해 안전한 통신(Secure Communication)을 수행하는데 요구되는 네트워크 보안 시스템의 일반적인 내용과 ATM Forum의 ATM 보안 프레임워크 1.0를 간단히 요약한다.

■ Authentication(인증)

인증은 ATM 커넥션이 시작될 때, 발신자의와 착신자 사이에서 서로 상대를 확인하는 보안 서비스이다. 이 서비스는 Impersonation이나 Spoofing 위협에 대한 방어로 이용되며, 안전한 커넥션 제공을 위해 필수적이다. 특히 안전한 키 교환 및 보안 협상 파라미터 교환을 위해 필요하며, 인증은 통신하는 상대의 상호 인증 혹은 편측 인증이 있다.

■ Confidentiality(기밀성)

기밀성은 인가되지 않은 사용자에 의한 데이터 유출을 보호하기 위한 서비스로, ATM 네트워크에서는 고정된 길이의 셀을 사용하므로, AAL 계층에서보다 셀 레벨에서 기밀성 서비스를 제공하는 것이 효율적인 암호화가 된다. 또한 셀의 페이로드만 암호화하면, 중간 노드에서는 셀 헤더의 복호화 없이 스위칭 되기 때문에 암호화에 따른 지연을 막을 수 있다. ATM 데이터의 암호화는 고속화가 가능한 대칭 알고리즘을 사용한다.

■ Integrity(무결성)

무결성 서비스는 데이터 Origin 인증의 일종으로, 데이터 값이나 데이터 값의 순서의 변경 및 악의의 데이터 변형에 대해 검출하는 서비스이다. ATM 네트워크에서는 종단점에서 이루어지며, 주로

AAL3/4과 AAL5의 AAL-SDU(Service Data Unit)에서 제공된다.

■ Non-repudiation(부인봉쇄)

부인 봉쇄는 사용자가 서비스 혹은 데이터를 액세스하였다는 사실을 부인할 수 없도록 하는 서비스이다.

ATM 네트워크에서는 안전한 통신을 위해서 부인 봉쇄 이외에 적어도 위어서 언급한 3가지 조건은 만족되어야 한다. 그리고 네트워크에 대한 안전한 시스템은 사용자의 접근제어와 Secure Key 관리(분배) 등과 같은 네트워크 보안 시스템이 필요하다. 키 관리는 보안시스템의 기본이 되는데, 키는 암호화(encryption)/복호화(decryption)용으로 사용되기 때문에 보안이 요구된다. 키의 관리나 분배는 여러 사용자가 사용하기 때문에 수동으로 하기는 힘들고, 네트워크를 통해서 자동 또는 반 자동으로 수행된다. 따라서 키가 공격 당하기 쉬우므로, 커넥션 설정 시에 교환되는 키에 대한 인증이 필요하다.

2.1 ATM 네트워크을 위한 일반적인 보안 목적

보안에 대한 목적을 고객 즉 서비스 가입자와 사용자, 네트워크 운용자와 서비스 제공자, 공동체 등의 관점에서 정리하면 다음과 같다.

■ 고객의 목적 :

고객은 보안에 대해 서로 다른 목적을 가지기 때문에 동일하지 않다. 따라서 다음과 같은 특성을 제공할 수 있는 보안 서비스가 요구된다.

- 서비스 가입, 활성화(Activation) 및 비활성화(Deactivation)의 가용성과 기능
- ATM 네트워크 서비스의 가용성과 기능
- 정확하고 검증이 가능한 요금체계
- 데이터의 무결성 및 데이터의 기밀성/사생활 (Privacy) 보장
- 익명으로 서비스 사용 등

■ 운용자의 목적:

네트워크 운용자와 서비스 제공자의 목적은 ATM 네트워크의 운용을 통해 좋은 수익을 올리는 것이다. 즉 네트워크 서비스의 공급으로 최대한 수익을 얻고, 인가되지 않은 사용자에 의한 네트워크 서비스의 경비 지출을 최소화 하는 것이다. 따라서 다음과 같은 사항이 요구된다.

- ATM 네트워크 서비스의 가용성과 기능
- ATM 네트워크 관리의 가용성과 기능
- 정확하고 검증이 가능한 요금체계 특히 사기 가능성이 없어야 함
- ATM 네트워크 서비스 사용 및 관리 활동에 대한 부인 봉쇄
- 모든 활동에 대한 책임성
- 데이터의 무결성과 데이터의 기밀성/사생활 보장

■ 공동 사회의 목적 :

주 목적은 ATM 네트워크 서비스의 가용성과 정확한 기능성, 데이터의 기밀성과 사생활 보장 등을 보증하는 것이다.

■ 기본 보안 목적:

이상에서 언급한 목적은 다음과 같은 보안 방법을 조합 또는 단독으로 설계, 구축함으로서 달성할 수 있다.

- 기밀성(Confidentiality)
- 데이터 무결성(Data Integrity)
- 책임성(Accountability)
- 가용성(Availability)

책임성(Accountability)은 주문한 모든 ATM 네트워크 서비스 또는 메니지먼트 행위를 개량화하

여 이의 행위에 대한 책임을 의미한다. 여기에는 인증과 부인봉쇄가 포함된다. 책임성은 서비스에 대한 용금 청구 및 시스템을 운용하기 위해서 운용자에게는 아주 중요하다. 가용성(Availability)은 합법적인 모든 엔티티(Entities)는 ATM 장비(ATM 교환기,스위치 등)을 액세스할 수 있어야 한다. 즉 서비스 거부 등이 일어나지 않도록 제공해 주어야 한다.

2.2 일반적인 위협 요소(Threats)

네트워크에서 위협 요소(Threats)는 보안 목적을 파괴할 가능성을 가지며, 그 종류는 일반적으로 크게 다음과 같이 분류된다.

- 원래부터 악의를 동반하지 않는 우연한 위협요소
- 보안 관리 결핍으로 야기되는 관리 위협요소
- 통신 혹은 망 자원을 공격할 목적으로 악의를 동반한 위협요소

이상의 위협 요소를 아래와 같은 카테고리내에서 분류하고, 이를 보안 목적에 대비하여 매핑하면 표1과 같다.

- Masquerade (Spoofing) (도용)
- Eavesdropping(도청)
- Unauthorized Access(비인가자 접근)
- Loss or Corruption of Information
- Repudiation(부인 봉쇄)
- Forgery(위조)
- Denial of Service(서비스 거부)

3. ATM 네트워크에서 보안 취약성 분석

3.1 ARP 서버의 취약점을 이용한 공격

ATM 기반 IP 통신에서는 IP 주소를 ATM 주소로 매핑시키는 과정이 필요하며, 이는 ATM ARP 서버를 통해 이루어진다. 먼저 LIS(Logical IP Subnetwork)내의 호스트는 자신의 IP 주소와 ATM 주소를 ARP 서버에 등록을 한다. 그리고 통신을 원하는 호스트는 상대 IP 주소를 가지고 ARP에 상대 ATM 주소를 조회하고, 이 ATM 주소를 이용하여 커넥션을 설정하고 설정된 커넥션으로 IP 통신을 한다. 이때 공격자가 IP 주소를 위조하여 위조된 IP 주소로 IP 패킷을 보내는 것이 가능하다. 이것을 IP Spoofing이라 하며, IP Spoofing 과정은 다음과 같다. ARP 서버는 정기적으로 ARP 테이블을 갱신하는데, 이때 공격 기회로 활용한다.

Main Security Objectives	Generic Threats						
	Masque-rade	Eaves-dropping	Un-authorized Acsess	Loss or Corruption of (transferred) Information	Repudiation	Forgery	Denial of Service
Confidentiality	×	×	×				
Data Integrity	×		×	×		×	
Accountability	×		×		×	×	
Availability	×		×	×			×

표 1. 보안 목적과 위협 요소간의 매핑

공격자는 ARP 서버의 ATM 주소를 미리 알고 있으며, 주소 등록과정은 다음과 같다. 공격자가 ATM ARP 서버에 커넥션을 설정하면, ARP 서버는 커넥션이 설정된 서버가 누구인가를 확인하기 위해, ARP는 In ATM ARP request 메시지를 단말로 보낸다. 이 메시지를 수신한 단말은 자신의 IP 주소와 ATM 주소가 포함된 In ATM ARP 메시지로 응답한다. ARP는 이 정보를 가지고 ARP 테이블을 변경한다. 이 때 공격자는 공격하고자 하는 IP 주소를 자신의 IP 주소로 등록하게 되면, 공격당한 IP 주소로 보낸 모든 정보는 공격자 단말로 전달될 것이다. 이 과정을 그림1에 나타냈다.

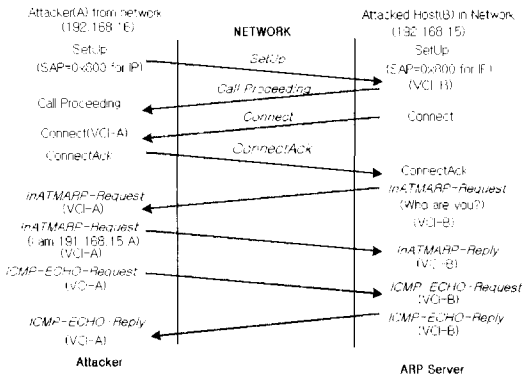


그림 1. IP Spoofing 과정

3.2 PNNI Routing 프로토콜을 이용한 공격

ILMI(Integrated Layer Management Interface)는 ATM 스위치와 단말기 사이의 인터페이스 역할을 수행하며, 이는 SNMP 프로토콜을 기반으로 하고 있다. 단말(예: Workstation)이 ATM UNI를 통해 ATM 네트워크에 접속하면, ILMI 메시지를 가지고 ATM 스위치와 통신하여 자동적으로 ATM 주소가 설정된다. 이때 보안 문제가 발생한다. 즉 SNMP가 간단한 인증절차를 제공하기 때문에, ILMI는 인증 절차를 제공하지 않는다. 따라서 공격자는 자신의 단말(예: Workstation)을 ATM 네트워크에 등록하기 위하여 ILMI 프로토콜을 사용한다. 공격자는 ATM 네트워크에 등록된 ATM 주소를 이용하여 스위치에 구성된 주소 Filter를 통과하는 것이 가능하다. 이때 공격자는 자신의 단말을 Offline된 단말의 ATM 주소로 등록할 수 있다. 또 ILMI는 ATM 스위치 단자에서 인터페이스 유형을 새롭게 구성할 수 있다. 이때 공격자는 단말이 접속된 인터페이스를 ILMI 프로토콜을 이용하여 NNI로 설정할 수 있다. 즉 스위치를 공격하기 위해 UNI 신호를 NNI 신호로 변경한다. 이러한 작업은 공격하기 전에 이루어 진다. 그러면 스위치는 공격자가 접속된 포트를 NNI로 인식하게 되며, 공격자 단말(Workstation)과 P-NNI 프로토콜로 통신하게 되므로, 공격자는 IP 정보를 가로챌 수 있다.

◈ 공격 시나리오:

ILMI 프로토콜에 의해 공격자가 접속된 인터페이스를 UNI에서 NNI로 변경하는 메커니즘을 나타낸다.

① Cold Start Trap 메시지를 스위치에 보낸다. ATM 스위치는 상대 Interface Management Entity(IME)의 재초기화로 인식하고, IME에 있는 이전의 MIB 정보를 지운다.

② ILMI 접속 절차가 수행되고, 상대 IME는 서로간의 연결 되었음을 확인한다.

③ ILMI는 자동적인 Configuration 절차를 수행한다. 스위치는 MIB의 객체에 의해 상대 IME의 형태를 다음과 절차에 의해 결정한다.

- atmfAtmLayerDeviceType object:공격자는 값2로 응답하여 네트워크 노드인척 한다.
- atmfAtmLayerNniSigVersion object : 공격자는 값3으로 응답해서 마치 P-NNI 라우팅 프로토콜을 사용하는 것처럼 가장한다.

3.3 망 자원 선점에 의한 서비스 거부

공격자가 ATM 네트워크 자원 선점에 의한 서비스 거부는 IP 주소, 대역폭, VPI 이나 VCI의 선점이 있다. ATM 망에서 VCI와 VPI는 UNI에서 각각 16비트와 8비트로 할당된다. 따라서 이들의 최대 할당비트는 2^{24}인데, 현실적으로 메모리의 크기나 보드 크기 등을 고려하여 최대 4096정도로 구현하고 있다. 따라서 공격자가 한 포트에서 VPI나 VCI를 모두 할당하여 선점하게 되면, VC 및 VP 부족으로 서비스가 거부된다. IP 주소의 선점은 LIS내의 ARP 서버의 주소 등록과정에서 일어날 수 있다. 공격자는 미 사용중인 IP 주소를 ARP 서버에 의뢰하여 알아 낼 수 있다. 이 공격은 ARP 서버가 LIS내에서 사용중인 IP 주소와 ATM 주소 테이블을 가지고 있다는 점에 착안한 것이다. 등록이 안된 IP 주소는 공격자가 ARP 서버에 의뢰할 때, ATM 주소 정보를 제공해 주지 못할 것이다. 따라서 공격자가 현재 사용하고 있지 않은 모든 IP 주소를 등록하게 되면, LIS내의 사용자는 IP 주소 부족으로 서비스를 받을 수 없게 된다. 또한 ARP 서버는 정기적으로 주소 테이블을 업데이트(update) 시킨다. 이때 오프라인된 IP 주소를 공격자가 등록하게 되면, 이 IP 주소를 사용하던 사용자는 서비스를 거부당하게 된다.

Native ATM에서 응용 서비스는 주로 CBR을 위해 VC(Virtual Channel)을 이용하며, IP 서비스는 ABR, UBR 채널을 이용하는 Best-effort 서비스이다. 따라서 CBR을 사용하는 서비스들은 ATM 네트워크에서 다른 트래픽보다 우선 순위를 갖는다. 만약에 Native ATM 서비스가 중계 스위치의 대역폭을 거의 점유하게 되면, 이 결과로 IP 트래픽은 대역 부족으로 서비스가 거부당하게 된다. 따라서 공격자가 미리 CBR 서비스에 대역폭을 예약해 두면, 시스템내의 대역폭이 공격자에 점유되어 다른 사용자들이 사용할 수 없게 된다. 이러한 공격은 현실적으로 매우 효과적이다. 원래 자원 예약은 ATM 네트워크에서의 일반적인 이루어지는 과정이므로, 만약 대역폭 부족으로 인해 클라이언트(호스트)가 서비스 거부를 당할 경우에 악의에 의한 공격인지, 일반적인 상황인지 판단이 어렵다.

3.4 ATM 특성으로 인한 공격 가능성

ATM 네트워크는 ATM 고유 특성으로 인해 다른 망에서는 발생하지 않는 위협요소가 있다. ATM 네트워크의 큰 장점인 QoS(Quality of service)의 보장은 서비스 등급에 따라 차등 서비스 제공이 가능한데, 이때 낮은 레벨의 서비스 등급자가 상대적으로 높은 레벨의 서비스 채널을 도용해서 사용할 가능성이 있다. 이를 채널 도용이라 한다. 그림 2와 같이 VC1이 VC2보다 높은 질(QoS)의 서비스를 제공 받는 채널이라 할 때, VC2 사용자가 VC1 채널을 도용하게 되면, VC1 사용자는 서비스를 못 받거나 서비스의 질이 떨어지게 된다. 이러한 공격은 양단의 스위치에서 라우팅 테이블 변경으로 가능하다. 이러한 발생은 동일 사업자가 제공하는 망에서는 가능성이 낮지만, 서로 다른 망 사업자간의 연동시에 일어날 가능성이 높다.

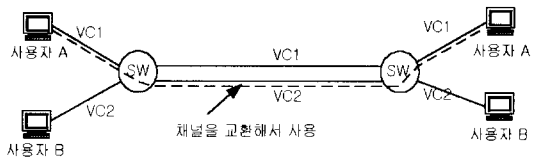


그림 2. ATM 네트워크에서의 VC 도용

또한 ATM망은 out of band 신호방식을 사용하므로, 사용자 채널로부터 논리적으로 분리된 별도의 신호용 VC를 이용한다. ATM망에서는 멀티 커넥션 호와 멀티 Party 호의 설정이 가능하다. 이를 위해서는 모든 호에 대해 Release와 Drop기능, 커넥션이나 Add Party기능이 수행되는데, 공격자

는 이러한 신호 기능을 이용하여 호 접속을 방해하는 것이 가능하다. 또한 멀티 커넥션이나 멀티 Party Call 커넥션 시에 사용자에 대한 인증이 없을 경우에 정보를 도청 당할 가능성이 높다.

그리고, ATM 스위치 내에는 자체적으로 고장 진단이나, 성능 관리 및 커넥션 관리 등의 기능이 있다. 이러한 기능은 TMN에 의해 구성관리, 안전 관리 등이 오프라인으로 수행된다. 또한 TMN은 독립적인 정보 Processing 시스템이므로 공격자가 TMN에 접근하여 스위치내의 주소 라우팅 테이블 값의 변경이 가능하다. 따라서 데이터를 다른 곳으로 유출시키거나 원래의 목적지에 도착하지 못하게 하여 서비스를 제공 받지 못하게 할 수도 있다. 이러한 ATM의 특성을 이용한 공격은 앞으로 일어날 가능성이 높다.

3.5 ATM 기반 MPLS에서 위협

ATM 기반 MPLS 네트워크 구성은 그림 3과 같다. 그림 3에서 볼 수 있듯이 MPLS는 Edge LSR (Label Switching Router)와 ATM-LSR 사이에 라우팅을 위한 경로(VPI=0, VCI=32)가 설정되어 있다. 또한 LDP 프로토콜을 이용하여 각 LSR에서 Tag Binding을 생성한다.

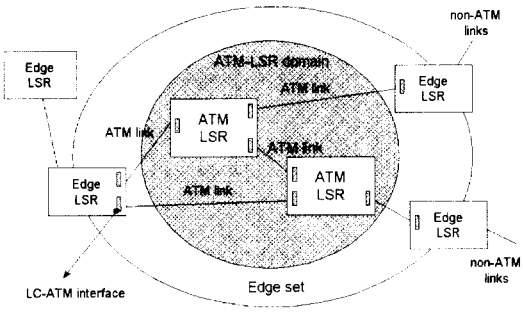


그림 3. ATM based on MPLS Network 모델

여기서 공격자는 LC-ATM 인터페이스를 장착하고, LDP 및 라우팅 프로토콜(OSPF)이 동작하는 워크스테이션을 ATM-LSR 혹은 Edge LSR으로 위장하여 동작하도록 할 수 있다. 즉, 공격자는 중간에서 IP 통신 내용을 가로챈다. 위장 ATM-LSR 혹은 Edge LSR을 이용하여 Tag Binding 정보의 변경도 가능하다. 또한 SIN(Ships-in-the-Night)모드로 동작할 때, MPLS에 할당된 VPI/VCI 공간을 다른 목적으로 할당하여 IP 서비스에 대해 거부가 발생하도록 만들 수 있다. 공격자에 의한 Binding 목적에 사용되는 TIB 테이블 내용 변경 등의 가능성도 있다.

4. ATM Forum의 보안 모델

ATM 보안 모델은 크게 보안 서비스 협상(Security Service Negotiation) 과 사용자 데이터 보호(User Data Protection)의 부분으로 나눌 수 있다. 보안 서비스 협상은 Security Service를 수행하려는 보안 주체(Security Agent) 상호간에 요구되는 보안 파라미터를 주고받는 메커니즘과 사용자 데이터 보호는 실제로 주고받는 데이터를 안전하게 통신할 수 있도록 하는 방법을 말한다.

보안 서비스 협상은 메시지를 전달하는 방식에 따라 나눌 수 있다. 즉 신호(Signaling) 메시지를 이용하여 협상하는 방법[ATM Forum, Dengs Solution, SAFE, Chuangs Solution], Management 정보(OAM Cell)를 통해 협상하는 방법[ATM Forum], In-band(Auxiliary) 채널을 통해 협상[ATM Forum, Stevenson]하는 방법으로 나눌 수 있다. 사용자 데이터 보호는 데이터를 비화(Encryption)하는 사용자 평면의 계층(Layer)에 따라 나눈다. 즉 ATM 계층에서 적용하는 방법 [ATM Forum, Stevensons Solution, Varadharajans Solution, Chuangs Solution]과 AAL 계층에서 적용하는 방법[Dengs Solution], AAL 상위 계층에서 적

용하는 방법[SAFE]으로 분류할 수 있다. 여기서는 ATM Forum 보안 모델을 중심으로 설명한다.

■ ATM Forum Solution Model

ATM Forum의 보안 모델을 설명하기 위해 그림4와 같은 상위 레벨의 기준 모델을 도입하고 있다. 그림 4에서 보면, ATM 네트워크의 양단에 종단시스템(End System:단말, 호스트 등)이 접속되어 있고, 양 단말간에 안전한 데이터(Secure Data)를 전달하기 위해서는 양 쪽에 SA(Security Agent)라는 엔티티가 존재한다. SA를 통해 양 단말에서 안전하게 데이터 전달에 사용할 보안 파라미터를 결정하고, 이 파라미터를 기본으로 하여 양 단말간에 데이터 전달이 이루어진다.

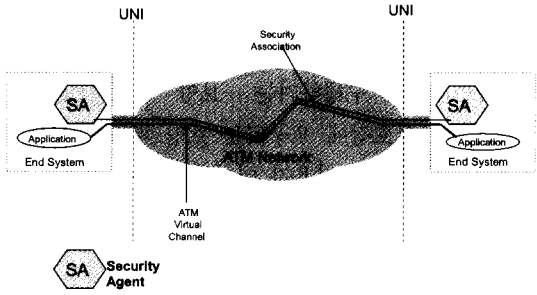


그림 4. ATM 종단시스템에서 SA간의 Security Association 모델

그림 4는 가장 대표적인 ATM 보안 시스템의 참조 모델로 ATM 네트워크를 사이에 두고 양 끝 단에 단말(End System)이 존재하며, 단말 내에 SA(Security Agent)가 있다. 이 경우 양 끝 단에 있는 End system의 SA가 SSIE((Security Service Information Element)를 사용하여 보안 서비스를 협상하고, 이를 기반으로 안전한 데이터 전달을 위해 데이터의 기밀성 및 무결성 서비스를 제공한다.

SSIE는 SSIE 헤더와 SAS(Security Association Section)으로 구성되어 있고, SAS는 Security Message Exchange Data와 Label based Access Control의 두 가지 경우로 나눌 수 있다. SSIE는 ATM VC 호 설정 시에 ATM VC에 대해 보안 서비스를 제공하기 위해 SA(Security Agent)가 사용하는 정보이며 다음과 같은 5가지가 지원되고 있다.

1) Signaling Support for Security Message Exchange
2) In-Band Security Message Exchange
3) Multiple Nested Security Service
4) Proxy Security Agent
5) User Plane Security Services

SAS는 두 ATM SA(Security Agent) 사이에 하나의 SAS을 설정하는데 필요한 정보를 제공한다. SSIE 정보는 보안 메시지 교환을 위해 신호 채널 또는 In-band 채널을 통해 이루어진다. SSIE 헤더 포멧과 SAS 포멧을 그림5 및 그림6에

Bits								
8	7	6	5	4	3	2	1	Octets
0	0	1	0	0	0	0	1	
In-Band Message Type								1
In-Band Message Length								2 - 3
Security Services Information Element								
x	x	x	x	x	x	x	x	4
Information element identifier								
1	Coding		Information Element Instruction Field					
Ext	Standard		Flag	Reserved	Information Element Action Indicator			5

(A) In-Band 방식

8	7	6	5	4	3	2	1	Octets
Security Service Information Element								1
0	0	1	0	0	0	0	1	
Information element identifier								
1 Ext	Coding Stadard		Information Element Instruction Field					2
			Flag	Reserved	Information Element Action Indicator			
Length of Generic Identifier transport information element contents								3
Length of Generic Identifier transport information contents(continued)								4
Security Association Service Identifier								5

(B) Signaling 방식

그림 5. SSIE Header 포멧

나타냈다.

ATM Forum은 사용자 데이터 셀 스트림에서 동기화 Security 정보가 요구될 때, OAM 채널을 사용하여 세션키를 교환한다. 이 세션키는 두 단계로 이루어진다. 첫번째는 Initial 세션키를 Security Agent 사이에 전송하는 것이고, 두번째는 이 키를 사용하여 사용자 데이터 셀 전송시 암호화할 새로운 세션키를 생성 교환하는 것이다. OAM 셀은 새로운 세션키 교환 및 VC 커넥션 설정시에 세션키 변경(Update) 알고리즘을 협상과 마스터 키를 교환하는데 사용된다.

SA사이에 메시지 교환 방식은 2-Way 보안 메시지 교환 및 3-Way 보안 메시지 교환 방식이 있다. 그림 5 및 그림 6의 포멧을 이용하여, PVC 방식은 3-Way 방법, SVC 방식은 2-Way 방법으로 보안 메시지 교환하고 있다. 특히 In-Band 방식의 FLOW 메시지를 구성할 경우에는 그림 5(A)와 같이 포멧 전단에 In-Band Message Type을 나타내는 1 Byte와 In-Band 메시지 길이 표시를 나타

Bits 8	7	6	5	4	3	2	1	Octets
Security Association Service Identifier								*5*
Security Association Section Length								5.1
Security Association Section Length (cont.)								5.2
Version			Transport Ind.		Flow Indicator		Discard	5.3
Scope								5.4
Scope								5.5
Relative ID								5.6
Relative ID								5.7
Target Security Entity Identifier								5.8
Security Service Data Section								*5.9*

Bits 8	7	6	5	4	3	2	1	Octets
0	0	1	0	0	1	x	x	
						SME Type		5.9
Security Message Exchange Format								
Security Entity Identifier								5.9.1
Security Service Specification *Section*								5.9.2
Confidentiality *Section*								5.9.3
Authentication *Section*								5.9.4

그림 6. SSIE Information 포멧

내는 2 Byte가 첨가된다.

특히 SVC 방식에서 SA간 보안 메시지 협상 중 가장 자연스러운 방식은 ATM 커넥션 중에 이루어지는 것이다. 이때 적용 가능한 방법은 2-Way 프로토콜 방식을 사용하며, 개념도는 그림7과 같다. UNI 4.0 신호를 이용하여 3-Way 보안 메시지 교환이 가능하게 되면, 사용자의 입장에서 보안 정책에 따라 다양한 방식을 선택할 수 있는 기회를 가질 수 있다.

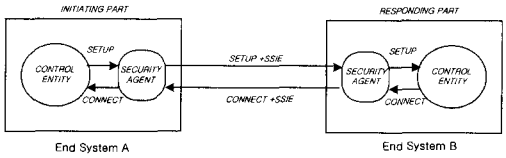


그림 7. 제어 엔티티와 시큐리티 에이전트와의 관계

ATM UNI 4.0 신호 방식에 의해 ATM 커넥션이 이루어질 때, 양 단말사이에 전달되는 신호메시지는 SETUP, CONNECT의 2종류 뿐 이다. 그러므로 양 단말에서 커넥션 설정 동안에 보안 메시지를 전달하는 방법은 Calling Party에서 Called Party로는 SETUP를 이용하고, Called Party에서 Calling Party로는 CONNECT를 이용한다. UNI 4.0 신호방식을 이용하면, 원천적으로 2-Way 보안 메시지 교환만 가능하다. 그러나 신호 채널과 In-Band 채널을 이용한 Hybrid 방식을 이용하면, 3-Way 보안 메시지 교환이 가능하다. 즉 UNI 4.0 신호 메시지 내에서 2개의 보안 메시지 즉 FLOW1-3E, FLOW2-3E를 교환하고, 커넥션 설정 후 In-Band 채널로 FLOW3-3E과 CONFIRM AP를 교환하는 방식이다. SA간에 FLOW2-3E의 메시지 교환이 이루어지면, 커넥션이 설정된다. 이때 SA는 사용자가 커넥션으로 데이터 전달이 되지 않도록 잠시 블로킹 시키고, In-Band로 남은 보안 메시지 교환을 수행하면 된다. 보안 메시지 교환이 성공적으로 이루어지면, 커넥션을 통해 Secure 데이터 전달이 되도록 블로킹을 해제한다. 이 방식의 보안 메시지 교환 절차를 그림8에 나타냈다.

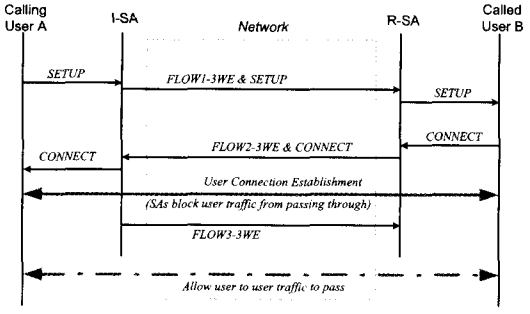


그림 8. UNI4.0 신호방식에 의한 3-Way 프로토콜 절차

5. ATM-WAN에서 사용자 데이터 모안 모델의 한 방법

5.1 사용자 유형별 데이터 보안 모델 분류

ATM Forum 모델은 ATM 보안을 위한 일반적인 모델로 정의되어 있으므로, 실제 시스템에 적용할 경우는 기술적, 경제적 등의 여러 측면을 고려해야 한다. 따라서 ATM Forum 모델을 기반으로 하여 사용자 유형별로 적용이 가능한 최적 보안 모델을 검토해 보고자 한다.

현재 ATM 기반 초고속통신망을 이용할 수 있는 사용자의 유형은 일반 가입자와 공공 기관, 기업 등으로 나눌 수 있다. 본 고에서는 ATM 네트워크를 이용하는 가입자를 사용자 유형별로 나누면, 다음과 같이 두 가지 경우를 생각할 수 있다.

① LAN을 갖는 기관 가입자가 ATM 네트워크를 백본망으로 접속하는 그룹
② 일반 가입자가 초고속 ATM 네트워크에 접속하여 서비스를 이용하는 그룹

초기 ATM 가입자는 상기 과 같이 각 기관의

LAN을 ATM 네트워크에 접속하여 각 기관별 CUG(Closed User Group)을 형성하는 경우가 대부분일 것이다. 이 경우에 각 기관이 갖는 LAN은 기존 LAN 가입자와 ATM LAN 가입자로 나누어 생각 할 수 있다. 현재 대부분이 기존의 LAN(Ethernet, FDDI 등)를 갖는 가입자일 것이다. 그러면 LAN간 접속은 그림9와 같이 ATM 네트워크를 통해 SVC 또는 PVC로 접속된다.

따라서 기관 가입자는 공중망 성격의 ATM 네트워크를 통해 종래와 같은 전용선 개념의 독자 네트워크를 구축하게 된다. 그러므로 기관 가입자는 전용선 개념과 똑같은 네트워크 보안을 유지하기를 원한다. 다른 유형의 일반 가입자도 ATM 네트워크에 접속하여 인터넷 서비스를 제공 받을 수 있다.

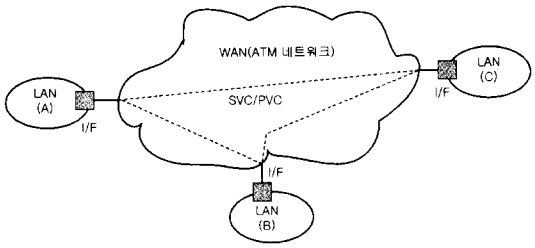


그림 9. ATM 네트워크를 이용한 LAN간 접속 예

본 고에서는 ATM 네트워크에 접속되어 있는 기관 가입자의 원격 사이트간에 정보 보안을 제공하는 모델에 대해서만 논 하기로 하고, 다음과 같은 조건을 가정한다.

① LAN 형태를 종래의 LAN 가입자와 ATM LAN 가입자로 2가지 유형만 고려한다.
② LAN간 접속은 SVC 혹은 PVC로만 가정한다.
③ 보안 서비스 적용 범위는 초고속 ATM 네트워크 내부로 한정하는 것을 원칙으로 한다.
④ Security Agent는 I/F(Interface Module) 모듈 또는 ATM-LAN 스위치 내에 둔다.

■ PVC 방식으로 접속된 경우

① 각 SA간에는 Security Service 협상은 커넥션(VC:Virtual Channel) 설정 후, In-band 방식에 의해 사전에 협상한다. 세션키 교환 및 변경은 OAM 채널을 통해서 이루어진다.
② 각 LAN의 SA들 사이에서, SA가 Initiator인지 Responder인지는 네트워크 메니지먼트가 각 SA에게 알려준다.

■ SVC 방식으로 접속된 경우

① 각 SA간에는 Security Service 협상은 커넥션 설정 중 또는 후에 각각 신호채널 및 In-band 방식으로 협상되어 진다. 또 세션키 교환 및 변경은 OAM 채널을 통해서 이루어진다.
② Calling Party 측의 SA가 Initiator가 되고, Called Party 측의 SA가 Responder가 된다.

5.2 모델별로 적용 가능한 사용자 데이터 보호 모델

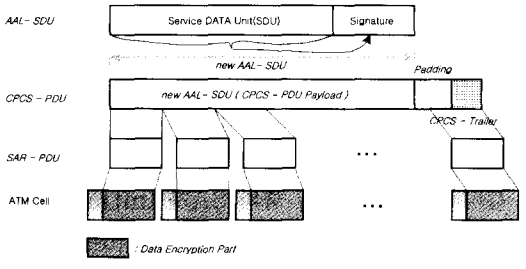
사용자의 데이터를 보호는 데이터 보호에 사용할 암호 알고리즘의 협상과 사용자 데이터의 암호화 부문으로 이루어진다. 그리고 사용자 데이터 보호를 위한 네트워크 보안 모델이다. 여기서는 WAN 환경의 ATM 네트워크에 접속되어 있는 기관 가입자에게 원격 사이트간에 정보보안을 제공하는 모델만 고려한다.

■ 기존의 LAN 가입자

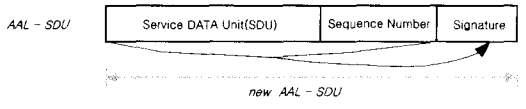
기존의 LAN 가입자가 ATM 네트워크을 이용한 VPN 모델은 그림 10과 같이 상상 할 수 있다. 이 모델은 I/F 장치에서 패킷 형태의 사용자 데이터가 ATM 셀 형태로 변환된다. 이때 변환 방법은 AAL

계층의 오버 헤드를 고려하여 AAL5를 이용하여 패킷을 ATM 셀로 처리한다고 가정한다. 따라서 사용자 데이터의 기밀성은 셀 레벨에서 수행하기로 하고, 무결성은 AAL 레벨에서 수행하기로 한다. ATM 계층에서는 하드웨어로 고속으로 처리할 수 있도록 기밀성을 제공할 수 있다.

그림 10. 기존 LAN가입자의 접속 방법



(A) Integrity without replay/reordering protection



(B) Integrity with replay/reordering protection

그림 11. AAL-SDU 레벨에서 데이터 무결성 제공 방법

단말에서 출발한 IP 패킷이 I/F 모듈에 도착하면, SA 간 보안 서비스 협상에서 얻은 파라미터를 이용하여 디지털 서명을 수행한다. 그림11(A)는 Replay 및 Reordering 방지 기능이 없이 데이터 무결성을 제공하는 방식으로, AAL-SDU 메시지가 입력되면 AAL-SDU를 통해 디지털 서명한 값을 AAL-SDU 끝에 붙인다. 이것은 새로운 AAL-SDU가 되며, CPCS-PDU로 변환된 다음에 48byte의 SAR-PDU 정보를 만든다. SAR-PDU정보에 셀 헤더를 부착하여 ATM 셀을 구성한다. 이때 ATM 셀 헤더의 PTI 필드를 이용하여 AAL-SDU 정보의 첫번째 셀 및 연속 셀, 그리고 마지막 셀 정보라는 것을 표시한다. 이와 같이 하는 이유는 수신 시에 송신과 똑같은 한 개의 완전한 패킷을 구성하기 위한 것이다. 다른 방법으로 Replay 및 Reordering 방지 기능을 갖는 방법으로는 그림11(B)와 같이 AAL-SDU를 구성하고, (A)와 같은 방법으로 ATM 셀화 처리를 하여 전달한다. 기밀성은 SAR-PDU에 대해 Encryption을 수행하면 된다.

■ ATM LAN 가입자

ATM-LAN 가입자가 ATM 네트워크을 이용한 VPN 모델은 그림12와 같이 구성할 수 있다.

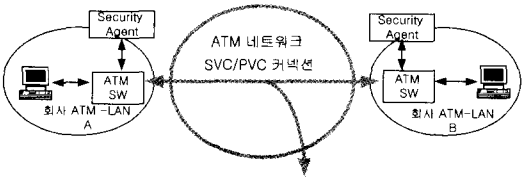


그림 12. ATM-LAN 가입자의 접속 방법

그림12와 같은 ATM LAN 가입자인 경우에는 기존의 LAN가입자와 동일하게 각 Security Agent 사이에서 보안 메시지 교환을 신호 채널 및 In-band 채널로 수행할 수 있다. 하지만 사용자 데이터 보호 관점에서 보면 약간의 차이가 있다. 그림12의 모델은 ATM LAN이 ATM 네트워크에 접속되어 있는 경우이므로, ATM LAN에 접속되는 단말은 ATM-LAN 접속 카드를 장착하고 있다. 즉 단말에서 데이터가 ATM 셀로 되어 ATM-LAN 스위치에 입력된다. 따라서 Security Agent는 ATM-LAN 스위치에 접속되어 있으므로 사용자

데이터 채널의 보안은 ATM 네트워크를 통한 ATM-LAN 스위치 사이에서 이루어진다.

따라서 사용자 데이터의 기밀성 제공은 ATM 셀 레벨(SAR-PDU)에서 이루어지므로 제공이 가능하다. 그러나 데이터 무결성은 AAL-SDU 레벨에서 이루어지므로 ATM -LAN 스위치간에서는 불가능하다. 즉 ATM-LAN 스위치는 셀 레벨에서 교환이 이루어지므로 단말에서 발생한 ATM 셀을 ATM-LAN 스위치에서 셀을 분해하지 않는 한 무결성 서비스 제공은 어렵다. 그러므로 ATM-LAN 스위치에서 셀을 분해하여 무결성 서비스를 제공한 후, 다시 셀화 하는 것은 무의미하다. 그러면 다음과 같이 두 가지 경우를 생각 할 수 있다.

① 데이터 무결성 서비스를 제공하지 않는 경우
② 데이터 무결성 서비스를 제공하는 경우

① 번의 경우는 데이터 기밀성 서비스만 제공함으로 SAR-PDU 레벨에서 수행 가능하다. 이는 양측의 Security Agent에서 이루어진다. ②번의 경우는 그림 13과 같이 ATM-LAN에 접속한 각 단말에 보조 Security Agent(A-SA)를 두고, ATM-LAN 스위치에 있는 M-SA(Main-SA)를 두는 방식으로 구성하면 가능하다. 이때 두가 방식을 생각 할 수 있다.

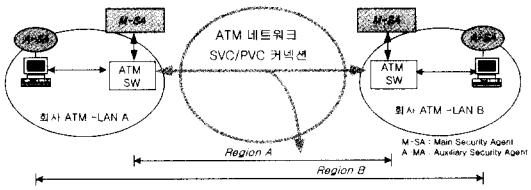


그림 13. Nesting 개념을 적용한 데이터 보안 방법

첫째, 원격지에 있는 단말과 통신을 할 경우, 단말에 있는 A-SA는 ATM-LAN 스위치에 있는 M-SA에 보안 메시지 협상을 의뢰하고, 그 결과만 받는다. 이렇게 구성하면 데이터 무결성은 단말간(Region B)에 해결하고, 데이터 기밀성은 M-SA 간(Region A)에서 해결이 가능하다. 둘째 데이터 기밀성과 무결성을 단말간(Region B)에서 해결하는 방식이다.

6. 결 론

지금까지 ATM 네트워크 보안에 대한 일반적인 사항과 ATM Forum 보안 모델을 중심으로 ATM 보안에 대해서 개략적으로 정리하고, 사용자 데이터 보호를 위한 한 방법으로 가입자 유형별 보안 모델을 중심으로 검토하였다.

금후 WAN ATM 시큐리티 분야에서 다루어질 주요 사항은 WAN 서비스를 보호하는 것이 주목적일 것이다. 따라서 ATM PVC 서비스 인 경우는 네트워크 메니지먼트 보안 분야에 주 관심을 가질 것이다. ATM SVC 서비스의 경우는 WAN 환경에서 CUG(Closed User Group) 서비스를 제공하는 것이다. 이 서비스는 암호화 기반에서 ATM 호 접근 제어 방식을 이용하여 제공하는 기술이다. ATM 서비스 거부 및 신호 변경 등의 위협에 대응하기 위해 ATM 제어평면에 대한 보호 방법과 ATM 라우팅 및 라우팅 정보 변경에 대응한 보호 방법 등이다.

네트워크 보안에서 중요하게 다루어질 분야는 ATM 네트워크의 가용성(Availability)과 무결성(Integrity), 비밀성(Privacy) 등이다. 네트워크 가용성은 네트워크 Failure에 대한 보호 및 검출 등을 통해 네트워크의 가용성 증대 방안에 관한 연구이며, 네트워크 무결성은 네트워크내에서 악의에 의한 물리적 기능적 변경에 대한 완벽한 대응을 말한다. 또 네트워크내에서 전달되는 데이터나 보관하는 데이터에 대해 보호를 제공해 주는 방법에 대한 연구 등이다.

※참 고 문 헌

[1] ATM Forum Technical Committee, ATM Security Frame-work 1.0 February 1998.

[2] ATM Forum Technical Committee, ATM Security Specification version 1.0, February 1999.

[3] Laurent M., Paul O. and Rolin P., Securing communications over ATM networks,IFIPSEC97, Copenhagen, Denmark, May, 1997.

[4] Stevenson D., Hillery N. and G. Byrd, Secure Communications in ATM Networks:, Communications of ACM, vol. 38, February 1995.

[4] J.CASE, M.Fedor, M.Schoffstall, J.Davin : A Simple Network Management Protocol : IETF RFC1157;May 1990.

[5] K. McCloghrie, M.Rose : Management Information Base for Network Management of TCP/IP-based internets : IETF RFC 1156, May 1990.

한 치 문

1977년 2월 경북대학교 전자공학과(공학사)
1983년 8월 연세대학교 대학원 전자공학과(공학석사)
1990년 9월 The University of Tokyo(동경대) 전자정보공학과(공학박사)
1977년2월~1983년3월 한국과학기술연구원(KIST) 연구원
1983년4월~1997년2월 한국전자통신연구원(ETRI) 선연, 책연 교환기술연구단 계통연구부장 역임
1997년3월~현재 한국외국어대학교 전자공학과 교수
※관심분야:ATM 통신망 및 교환, IMT-2000 네트워크, 네트워크 보안 등

김 기 현

1993년 2월 경북대학교 전자공학과(공학사)
1995년 2월 경북대학교 전자공학과(공학석사)
1995년 7월~1996년 7월 데이콤 시외전화구축팀
1996년 7월~현재 한국정보보호센터 시스템기술팀 선임연구원
※관심분야:침입탐지, 네트워크 보안

김 홍 근

1985년 2월 서울대학교 컴퓨터공학과(공학사)
1987년 2월 서울대학교 컴퓨터공학과(공학석사)
1994년 2월 서울대학교 컴퓨터공학과(공학박사)
1994년 5월~1996년 5월 한국전산원 전산망보안팀장
1996년 5월~현재 한국정보보호센터 시스템기술팀장
※관심분야:컴퓨터보안, 병렬알고리즘