ATM Network 보안 기술과 데이터 보호 방법

장 종 현[†] · 한 치 문[††] · 이 동 길[†††]

요 약

ATM은 고속통신 네트워크를 구현하기 위하여 요구에 따라 대역폭의 확장을 통한 망 자원의 효율성과 융통성을 제공한다. ATM은 서로 다른 서비스 품질을 필요로 하는 음성, 비디오, 이미지 및 데이터를 포함하는 다양한 응용을 지원한다. ATM Forum 보안 그룹은 ATM 네트워크에 대한 보안 서비스를 정의한 보안 규격을 발표하였다. 본 논문에서는 ATM 네트워크 보안 기술에 대한 일반적인 요구 사항과 ATM 네트워크에서 보안의 취약성을 분석하고, ATM Forum을 중심으로 한 ATM 보안 모델을 소개하고, 초고속통신망(ATM-WAN) 환경에 적용할 수 있는 ATM 네트워크 접속 모델 및 서비스 이용자 유형별 사용자 데이터 보호 모델을 소개하고 시뮬레이터를 이용하여 암호 알고리즘에 따른 데이터 전달 특성을 분석한다.

ATM Network Security Technology and Data Protection Method

Jong-Hyun Jang[†] · Chi Moon Han[††] · Dong Gil Lee[†††]

ABSTRACT

Asynchronous Transfer Mode (ATM) is seen to be a technology that allows flexibility, efficiency and manageable bandwidth on demand to be achieved in high-speed networks. ATM is able to support a variety of applications including voice, video, image and data with different quality of service requirements. The ATM Forum Security Working Group proposed that security specification, which defines security services for the ATM networks. This paper describes an overview of ATM security as specified by the ATM Forum Security Working Group. This Paper present a fundamental analysis of the ATM networks security, leading to a systematic of every weakness in ATM networks that may be exploited by security attacks. We introduce ATM security Model on focus ATM Forum and one method of data protection and analyze data transfer property in the ATM-WAN environments.

1. 서 론

최근 인터넷은 새로운 멀티미디어 응용 서비스 개발에 힘입어 음성 및 영상과 같은 스트림 형태(stream type) 서비스를 수용하는 방향으로 전개되면서 네트워크 하부 네트워크 구조도 ATM 망을 기반으로 하여 진행되고 있다. ATM 네트워크는 음성, 데이터, 비디오 등의 서비스를 통합하여 전달 교환하는 멀티미디어 네트워크이다. ATM 네트워크는 기본적으로 연결형(Connection-Oriented) 통신을 하는 구조인 반면, 기존의 인터넷은 비연결형 통신 방식을 취하고 있다. 그러므로 ATM 네트워크에서 비연결형 데이터를 효율적으로 제공하기 위하여 CLIP(Classical IP), LANE, MPOA 등의 다양한 방식이 연구되고 있다. 한편 IP 교환을 Cut-through 형태로 취급하는 IP Switching 방식에

† 준 회 원 : 한국전자통신연구원 교환전송기술연구소 선임연구원
†† 정 회 원 : 한국외국어대학교 전자공학과 교수
††† 정 회 원 : 한국전자통신연구원 책임연구원
논문접수 : 2000년 5월 30일, 심사완료 : 2000년 8월 7일

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 공유하는 매체 공유형의 액세스 형태로 구성되며, 고속 버스트성의 트래픽이 주류를 이루고 있다. 이처럼 한 개의 가입자 회선을 다양한 사용자가 공유하는 ATM 네트워크를 통해 특정 그룹별로 전용 네트워크를 구축할 필요가 있는데, ATM 네트워크를 기반으로 논리적으로 서로 다른 VPN(Virtual Private Network) 구축하여 정보 전달을 시도하고 있다. 따라서, 동일한 인프라에서 서로 다른 VPN이 공존함으로 VPN간의 정보 누설 또는 도청의 위협에 대한 대책이 요구된다.

ATM 네트워크에서 보안의 중요성이 인식되어 ATM Forum를 중심으로 ATM 데이터 전달에 대한 보안의 표준화가 진행되어 1998년 12월에 ATM Security Version 1.0이 발표되었다. ATM 네트워크에 보안 기술의 기본 개념은 네트워크 프로토콜 모델을 변경하지 않고 구현할 수 있는 보안 모델과 최소한의 비용(Overhead)으로 보안 성능을 유지할 수 있는 보안 모델이어야 한다.

본 고에서는 ATM 네트워크 보안 기술에 대한 요구사항과 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 데이터 통신을 위한 네트워크 보안 시스템의 일반적인 내용과 ATM Forum의 ATM 보안 프레임워크 1.0를 간단히 요약한다 [1, 3].

- Authentication(인증)

인증은 ATM 연결이 시작될 때, 발신자와 착신자 사이에 상대방의 신원을 확인하는 보안 서비스이다. 이 서비스는 Impersonation이나 Spoofing 위협에 대한 방어로 이용되며, 안전한 연결 제공을 위해 필수적이다. 특히 안전한 키 교환 및 보안 협상 파라미터 교환을 위해 필요하며, 인증방법으로는 통신하는 상대방에 대한 인증과 상호 인증이 있다.

- Confidentiality(기밀성)

기밀성은 인가되지 않은 사용자에 의한 데이터 유출을 보호하기 위한 서비스로써 ATM 네트워크에서는 고정된 길이의 셀을 사용하므로, ATM 계층에서 셀 단위의 기밀성 서비스를 제공하는 것이 효율적인 암호화가 된다. 왜냐하면 ATM 셀의 페이로드만 암호화하면, 중간 노드에서는 셀 헤더의 복호화 절차없이 전달되기 때문에 암호화에 따른 지연을 최대한 방지할 수 있다. ATM 데이터의 암호화는 고속화가 가능한 대칭형 스트림 암호화 알고리즘을 사용한다.

- Integrity(무결성)

무결성 서비스는 데이터 발신지 인증의 일종으로, 전달과정에서 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 부인봉쇄를 제외한 인증, 기밀성, 무결성 기능을 만족하기 위하여 사용자의 접근제어와 암호키 관리(분배) 등과 같은 네트워크 보안 시스템이 필요하다. 암호키 관리는 보안시스템의 기본이 되는데, 암호키는 암호화/복호화에 사용되며 여러 사용자가 사용하기 때문에 키분배는 네트워크를 통해서 전달되며, 암호키는 해커로부터 공격 당하기 쉬우므로, 연결 설정 과정에서 교환되는 키에 대한 인증이 필요하다.

2.1 ATM 네트워크을 위한 일반적인 보안 목적

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

2.1.1 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 비활성(De-activation)의 가용성과 기능
- ATM 네트워크 서비스의 가용성과 기능
- 정확하고 검증이 가능한 요금체계
- 데이터의 무결성 및 데이터의 기밀성/프라이버시 보장
- 익명으로 서비스 사용 등

2.1.2 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

2.1.3 공동 사회의 목적

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

2.1.4 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)

책임성은 주문한 모든 ATM 네트워크 서비스 또는 관리 행위에 대한 책임을 의미한다. 여기에는 인증과 부인봉쇄가 포함된다. 책임성은 서비스에 대한 과금 및 시스템을 운용하기 위해서 운용자에게는 아주 중요하며, 가용성은 합법적인 모든 개체는 ATM 장비(ATM 교환기, 스위치 등)를 액세스할 수 있어야 한다. 즉 서비스 거부 등이 일어나지 않도록 제공해 주어야 한다.

2.2 일반적인 위협 요소(Threats)

네트워크에서 위협 요소는 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 범주내에서 분류하고, 이를 보안 목적에 대비하여 매핑하면 <표 1>과 같다.

- Masquerade (Spoofing)(도용)
- Eavesdropping(도청)
- Unauthorized Access(비인가자 접근)
- Loss or Corruption of Information(정보 파괴/손실)
- Forgery(위조)
- Denial of Service(서비스 거부)

〈표 1〉 보안 목적과 위협 요소간의 매핑

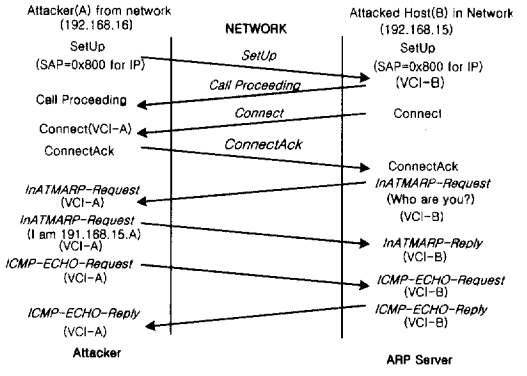
주요 보안 목적	일반 위협(Generic Threats)					
	위장	도청	비인가 접근	정보 훼손	위조	서비스 거부
기밀성	×	×	×			
무결성	×		×	×	×	
책임성	×		×		×	
가용성	×		×	×		×

3. ATM 네트워크에서 보안 취약성 분석

3.1 ARP 서버의 취약점을 이용한 공격

ATM 기반의 IP 통신에서 ATM ARP 서버를 통하여 IP 주소를 ATM 주소로 매핑시키는 과정이 필요한데, 먼저 LIS(Logical IP Sub-network)내의 호스트는 자신의 IP와 ATM 주소를 ARP 서버에 등록하게 된다. 그리고 통신을 원하는 호스트는 ARP 서버로 상대방의

IP 주소에 대한 ATM 주소를 조회하고, 이 ATM 주소를 이용하여 연결을 설정하고 IP 통신을 한다. ARP 서버는 정기적으로 ARP 테이블을 갱신하게 되는데, 갱신 과정에서 위조된 IP 주소를 ARP 서버에 등록하여 공격하는 IP Spoofing 방법은 다음과 같다. 공격자는 ARP 서버의 ATM 주소를 미리 알고 있는 상태에서 공격자가 ATM ARP 서버에 연결을 설정하면, ARP 서버는 연결이 설정된 호스트를 확인하기 위해, ARP는 *In ATM ARP request* 메시지를 단말로 보낸다. 이 메시지를 수신한 단말은 위조된 주소와 ATM 주소가 포함된 *In ATM ARP* 메시지로 응답하면 ARP 서버는 해당 주소에 대한 ARP 테이블을 변경하게 되여 공격 당한 IP 주소로 보낸 모든 정보는 공격자 단말로 전달되게 하는 공격 방법으로 절차는 (그림 1)과 같다.



(그림 1) IP Spoofing 과정

3.2 PNNI Routing 프로토콜을 이용한 공격

ILMI(Integrated Layer Management Interface)는 SNMP 프로토콜을 기반으로 ATM 스위치와 단말기 사이의 인터페이스 역할을 수행하는데, 단말(예 : Workstation)이 ATM UNI를 통해 ILMI 메시지를 가지고 접속을 요청하면 ATM 스위치와 통신하여 자동적으로 ATM 주소가 설정되는 과정에서 보안 문제가 발생한다. 즉, ILMI 프로토콜이 인증 절차를 제공하지 않는 약점을 이용하여 ILMI 프로토콜을 사용하여 자신의 단말을 ATM 네트워크에 등록하기 위하여 ATM 네트워크에 등록된 ATM 주소를 이용하여 스위치에 구성된 주소 Filter를 통과하는 것이 가능하게 되어 공격자는 자신의 단말을 오프라인 상태의 단말의 ATM 주소로 등록할 수 있다. 또 ILMI는 ATM 스위치 단자에서 단말이 접속된 인터페이스를 ILMI 프로토콜을 이용하여 NNI로 인터페이스 유형을 새롭게 구성할 수 있으므로 공격자는 스위치를 공격하기 위해 UNI 신호를 NNI 신호로 변경한다. 그러면 스위치는 공격자가 접속된 포트를 NNI로 인식하게 되며, 공격자 단말과 P-NNI 프로토콜로 통신하게 되므로, 공격자는 IP 정보를 가로챌 수 있다.

공격자가 ILMI 프로토콜을 이용하여 UNI에서 NNI 인터페이스로 변경하는 메커니즘을 다음과 같다.

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 수행하는데 스위치는 MIB의 객체에 의해 상대 IME의 형태를 다음과 절차에 의해 결정한다.

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

3.3 망 자원 선점에 의한 서비스 거부

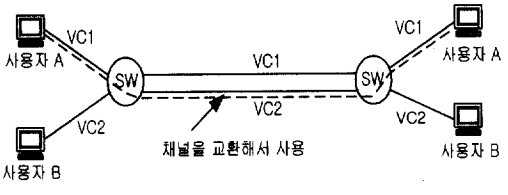
ATM 네트워크에서 자원 선점에 의한 서비스 거부 종류로는 IP 주소, 대역폭, VPI 및 VCI의 선점이 있다. ATM 망에서 VCI와 VPI는 UNI에서 각각 16비트와 8비트로 할당되어 이론적으로 최대 2^{24}개가 가능하지만 하드웨어 구현측면에서 통상 4,096정도로 구현하고 있다. 따라서 공격자가 한 포트에서 VPI나 VCI를 모두 할당하여 선점하게 되면, VC 및 VP 부족으로 서비스가 거부된다. 또한 IP 주소의 선점은 LIS내의 ARP 서버의 주소 등록과정에서 ARP 서버가 LIS내에서 사용중인 IP 주소와 ATM 주소 테이블을 가지고 있다는 점에 착안하여 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 갱신하게 되는데 이때 오프라인된 IP 주소를 공격자가 등록하게 되면, 이 IP 주소를 사용하던 사용자는 서비스를 거부당하게 된다.

Native ATM에서 응용 주로 가상채널을 이용한

CBR 서비스이며, IP 서비스는 ABR, UBR 채널을 이용하는 Best-effort 서비스이다. 따라서 CBR을 사용하는 서비스들은 ATM 네트워크에서 다른 서비스보다 높은 우선 순위를 갖게 되는데, 만약 Native ATM 서비스가 중계 스위치의 대역폭을 거의 점유하게 되면, IP 서비스는 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 사용자가 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 도용하는 사용하는 채널 도용의 가능성이 있다. (그림 2)와 같이 VC1이 VC2보다 높은 품질(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 채널 도용은 동일 사업자가 제공하는 망에서는 가능성이 낮지만, 서로 다른 망 사업자간의 망연동시 발생 가능성이 높다.



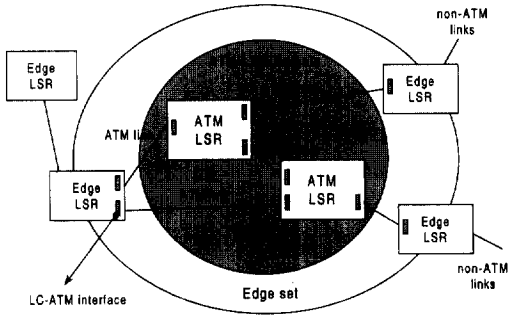
(그림 2) ATM 네트워크에서의 VC 도용

그리고, ATM 망은 데이터 채널과 신호 채널이 논리적으로 분리된 out of band 신호방식을 사용하므로 ATM 망에서는 다중연결 및 멀티 파티호의 설정이 가능하다. 이를 위해서는 모든 호에 대해 Release와 Drop 기능 및 Add Party 기능이 수행되는데, 공격자는 이러한 신호 기능을 이용하여 호 접속을 방해하는 것이 가능하다. 또한 다중 연결 및 멀티 파티호 연결시에 사용자에 대한 인증이 없을 경우에 정보를 도청 당할 가능성이 높다.

그리고, ATM 스위치 내에는 자체적으로 고장 진단이나, 성능 관리 및 연결 관리 등의 기능이 제공되는데, 이는 TMN에 의해 구성관리, 안전 관리 등이 오프라인으로 수행된다. 또한 TMN은 독립적인 정보 처리 시스템이므로 공격자가 TMN에 접근하여 스위치내의 라우팅 테이블 정보의 변경이나 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 3)과 같다. (그림 3)에서 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 위장 동작하게 하여 IP 통신 내용을 가로채거나 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 거부를 유

발하거나 Binding 목적에 사용되는 TIB 테이블의 변경도 가능하다.

4. ATM Forum의 보안 모델

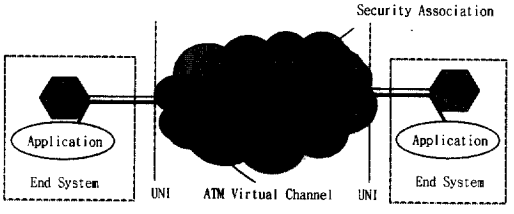
ATM 보안 모델은 크게 보안 서비스 협상(Security Service Negotiation)과 사용자 데이터 보호(User Data Protection)의 부분으로 나눌 수 있다. 보안 서비스 협상은 보안서비스를 수행하려는 SA(Security Agent) 상호간에 요구되는 보안 파라미터를 주고 받는 메커니즘을, 사용자 데이터 보호는 실제로 주고 받는 데이터를 안전하게 통신할 수 있도록 하는 방법을 말한다.

보안 서비스 협상은 메시지를 전달하는 방식에 따라 시그널링 메시지를 이용하여 협상하는 방법[ATM Forum, Deng's Solution, SAFE, Chuang's Solution], 관리 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 암호화(Encryption)하는 사용자 평면의 계층(Layer)에 따라 나눈다. 즉 ATM 계층에서 적용하는 방법[ATM Forum, Stevenson's Solution, Varadharajan's Solution, Chuang's Solution]과 AAL 계층에서 적용하는 방법[Deng's Solution], AAL 상위 계층에서 적용하는 방법[SAFE]으로 분류할 수 있다. 여기서는 ATM Forum 보안 모델을 중심으로 설명한다[3, 4].

4.1 ATM Forum Solution Model

ATM Forum의 보안 모델을 설명하기 위해 (그림 4)와 같은 상위 레벨의 기준 모델을 도입하고 있다. (그림 4)에서 보면, ATM 네트워크의 양단에 종단시스템(End System : 단말, 호스트 등)이 접속되어 있고, 양 단말간에 안전하게 데이터를 전달하기 위해서는 양쪽에 SA라는 개체가 존재한다. SA를 통해 양 단말에서 안전하게 데이터 전달에 사용할 보안 파라미터를 결정하고, 이 파라미터를 기본으로 하여 양 단말간에 데이터 전달이 이루어 진다.

(그림 4)는 가장 대표적인 ATM 보안 시스템의 참조 모델로 ATM 네트워크를 사이에 두고 종단에 단말이 존재하며, 단말 내에 SA가 있다. 이 경우 양 종단에 위치한 SA가 SSIE((Security Service Information Element)를 이용하여 보안 서비스를 협상하고, 이를 기반으로 안전한 데이터 전달을 위해 데이터의 기밀성 및 무결성 서비스를 제공한다.



(그림 4) ATM 종단시스템에서 SA간의 Security Association 모델

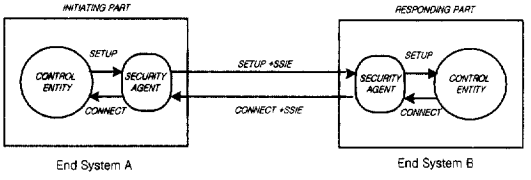
SSIE는 SSIE 헤더와 SAS(Security Association Section)으로 구성되어 있고, SAS는 Security Message Exchange Data와 Label based Access Control의 두 가지 경우로 나눌 수 있다. SSIE는 ATM VC 호 설정 시에 ATM VC에 대해 보안 서비스를 제공하기 위해 SA가 사용하는 정보이며, 다음과 같은 5가지가 지원되고 있다.

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

SSIE 정보는 보안 메시지 교환을 위해 신호 채널 또는 In-band 채널을 통해 이루어진다.

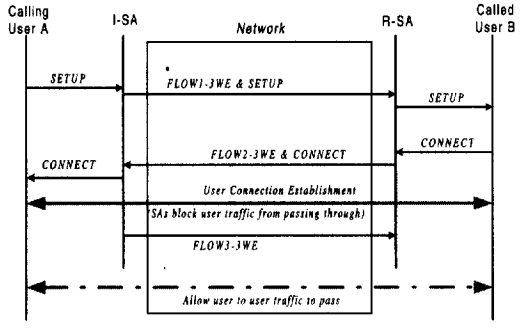
ATM Forum은 사용자 데이터 셀 스트림에서 보안 정보가 요구될 때, OAM 채널을 사용하여 세션키를 SA 사이에 교환하고, 이 키를 사용하여 사용자 데이터 셀 전송시 암호화할 새로운 세션키를 생성 교환하는 2단계로 이루어 진다. OAM 셀은 새로운 세션키 교환 및 VC 연결 설정시에 세션키 변경(Update) 알고리즘 협상과 마스터 키를 교환하는데 사용된다.

SA사이에 메시지 교환 방식은 2-Way 및 3-Way 보안 메시지 교환 방식이 있는데 SVC 방식에서 SA간 보안 메시지 협상은 ATM 연결 중에 (그림 5)와 같이 보안 메시지를 교환하고, PVC에서는 ATM UNI 4.0 신호를 이용하여 3-Way 보안 메시지 교환이 가능하여 사용자의 입장에서 보안 정책에 따라 다양한 방식을 선택할 수 있다.



(그림 5) 제어 개체와 보안 에이전트와의 관계

ATM UNI 4.0 신호 방식에 의해 ATM 연결이 이루어질 때, 양 단말사이에 전달되는 신호메시지는 *SETUP, CONNECT*이 있는데, 양 단말에서 연결 설정 동안에 보안 메시지를 전달하는 방법은 Calling Party에서 Called Party로는 *SETUP*를 이용하고, Called Party에서 Calling Party로는 *CONNECT*를 이용한다. UNI 4.0 신호방식을 이용하면, 원천적으로 2-Way 보안 메시지 교환만 가능하지만 신호 채널과 In-Band 채널을 이용한 Hybrid 방식을 이용하면, 3-Way 보안 메시지 교환이 가능하다. 즉, UNI 4.0 신호 메시지 내에서 *FLOW1-3E, FLOW2-3E*를 교환하고, 연결 설정 후 In-Band 채널로 *FLOW3-3E*과 *CONFIRM AP*를 교환하는 방식이다. SA간에 *FLOW2-3E*의 메시지 교환이 이루어지면, 연결이 설정된다. 이때 SA는 사용자가 채널로 데이터 전달이 되지 않도록 잠시 블로킹 시키고, In-Band로 남은 보안 메시지 교환을 수행하면 된다. 보안 메시지 교환이 성공적으로 이루어지면, 연결된 채널을 통하여 안전한 데이터 전달이 가능하게 된다. 이 방식의 보안 메시지 교환 절차를 (그림 6)에 나타냈다.



(그림 6) UNI4.0 신호방식에 의한 3-Way 프로토콜 절차

5. ATM-WAN에서 사용자 데이터 보안 모델링

5.1 사용자 유형별 데이터 보안 모델 분류

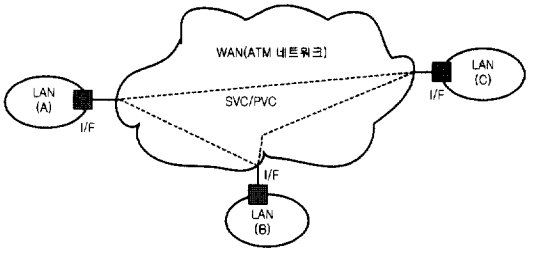
ATM Forum 모델은 ATM 보안을 위한 일반적인 모델로 정의되어 있으므로, 실제 시스템에 적용할 경우는 기술적, 경제적 등의 여러 측면을 고려해야 한다. 따라서 ATM Forum 모델을 기반으로 하여 사용자 유형별로 적용이 가능한 최적 보안 모델을 검토해 보고자 한다.

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 근거리통신망(LAN)을 갖는 기관 가입자가 ATM 네트워크를 백본망으로 접속하는 그룹
② 일반 가입자가 초고속 ATM 네트워크에 접속하여 서비스를 이용하는 그룹

초기 ATM 가입자는 상기 ①과 같이 각 기관의 LAN을 ATM 네트워크에 접속하여 각 기관별 폐쇄사용자그룹(Closed User Group)을 형성하는 경우가 대부분일 것이다. 이 경우에 각 기관이 갖는 LAN은 기존 LAN(Ethernet, FDDI 등)를 갖는 가입자와 ATM LAN 가입자로 구성되어 진다. 그러면 LAN간 접속은 (그림 7)과 같이 ATM 네트워크를 통해 SVC 또는 PVC로 접속된다.

따라서 기관 가입자는 공중망 성격의 ATM 네트워크를 통해 종래와 같은 전용선 개념의 독자 네트워크를 구축하게 되며 동일한 네트워크 보안을 유지하기를 원한다.



(그림 7) 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.

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

5.1.1 PVC 방식으로 접속된 경우

- 각 SA간에는 보안 서비스 협상은 가상채널 연결 설정 후, In-band 방식에 의해 사전에 협상한다. 세션 키 교환 및 변경은 OAM 채널을 통해서 이루어진다.
- 각 LAN의 SA들 사이에서, SA가 Initiator인지 Responder인지는 네트워크 관리자가 각 SA에게 알려준다.

5.1.2 SVC 방식으로 접속된 경우

- 각 SA간에는 보안 서비스 협상은 연결 설정 과정 또는 후에 신호채널 및 In-band 방식으로 협상되어 진다. 또 세션 키 교환 및 변경은 OAM 채널을 통해서 이루어진다.
- Calling Party 측의 SA가 Initiator가 되고, Called Party 측의 SA가 Responder가 된다.

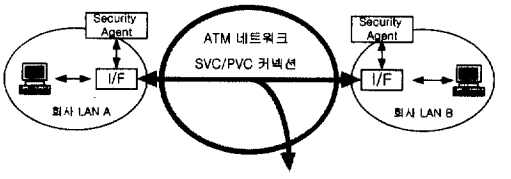
5.2 모델별로 적용 가능한 사용자 데이터 보호 모델

사용자의 데이터 보호에 사용할 암호 알고리즘의 협상과 데이터의 암호화 부분으로 이루어진 네트워크 보안 모델로써, WAN 환경의 ATM 네트워크에 접속되어 있는 기관 가입자에게 원격 사이트간에 정보보안을 제공하는 모델만 고려한다.

5.2.1 기존의 LAN 가입자

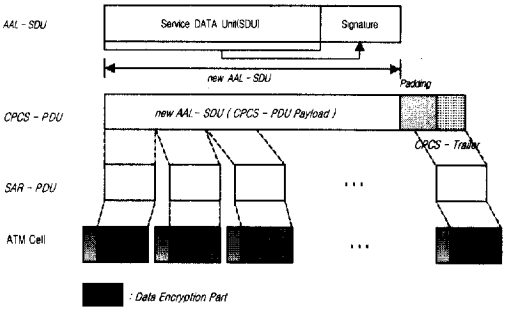
기존의 LAN 가입자가 ATM 네트워크을 이용한 VPN 모델은 (그림 8)과 같이 생각할 수 있다. 이 모델은 I/F 장치에서 패킷 형태의 사용자 데이터가 적응계층의 부하를 고려하여 AAL5 계층에서 ATM 셀로변환하여 처리한다고 가정한다. 따라서 사용자 데이터의 기밀성은 하드웨어로 고속으로 처리할 수 있도록 셀 레벨에서 제공하고, 무결성은 적응계층에서 수행한다.

단말에서 전달된 IP 패킷이 I/F 모듈에 도착하면, SA 간 보안 서비스 협상에서 얻은 파라미터를 이용하

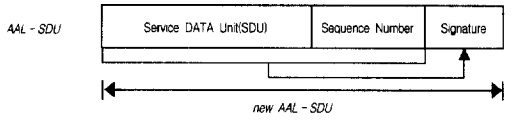


(그림 8) 기존 LAN 가입자의 접속 방법

여 디지털 서명을 수행한다. (그림 9(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 수신측에서 동일한 패킷을 구성하기 위한 것이다. 또 방법으로 Replay 및 Reordering 방지 기능을 갖는 방법으로는 (그림 9(B))와 같이 일정길이의 일련번호를 추가하여 AAL-SDU를 구성하고, (A)와 같은 방법으로 ATM 셀로 변환한 후 SAR-PDU에 대해 암호화하여 전달하면 수신측에서 도착된 메시지의 순서를 확인할 수 있다.



(A) Integrity without replay/reordering protection



(B) Integrity with replay/reordering protection

(그림 9) AAL-SDU 레벨에서 데이터 무결성 제공 방법

5.2.2 ATM LAN 가입자

ATM-LAN 가입자가 ATM 네트워크을 이용한 VPN 모델은 (그림 10)과 같이 구성할 수 있다.

(그림 10)과 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. (그림 10)의 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.

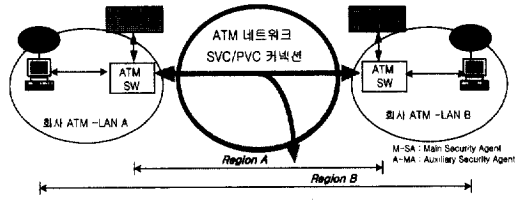
(그림 10) ATM-LAN 가입자의 접속 방법

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 해석하여 무결성 서비스를 제공한 후, 다시 셀로 분할하는 것은 무의미하다. 그러면 다음과 같이 두 가지 경우를 생각할 수 있다.

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

①의 경우는 데이터 기밀성 서비스만 제공함으로 SAR-PDU 레벨에서 수행 가능하다. 이는 양 측의 Security Agent에서 이루어진다. ②의 경우는 (그림 11)과 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 두 가지 방식을 생각 할 수 있다.

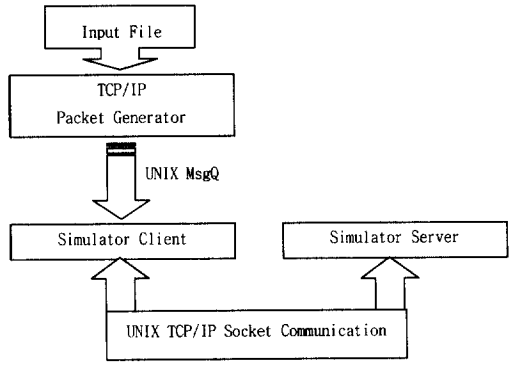
첫째, 원격지에 있는 단말과 통신을 할 경우, 단말에 있는 A-SA는 ATM-LAN 스위치에 있는 M-SA에 보안 메시지 협상을 의뢰하고 결과만 받는다. 이렇게 구성하면 데이터 무결성은 단말간(*Region B*)에 해결하고, 데이터 기밀성은 M-SA간(*Region A*)에서 해결이 가능하다. 둘째 데이터 기밀성과 무결성을 단말간(*Region B*)에서 해결하는 방식이다.



(그림 11) Nesting 개념을 적용한 데이터 보안 방법

5.3 사용자 데이터 보안 시뮬레이션

사용자 데이터 암호화 통신 기능을 수행하는 ASS는 (그림 12)와 같이 TCP/IP 패킷 생성기, ATM시뮬레이터 클라이언트와 서버의 3개의 프로세스로 구성된다. 패킷 생성기와 시뮬레이터 클라이언트와는 UNIX 메시지 큐 또는 소켓을 이용하여 프로세스간 통신이 이루어지며, 클라이언트와 서버 시스템간은 TCP/IP 소켓 통신을 이용한다. 암호 키 분배 방식은 시스템 시작 과정에서 세션 키를 전달하는 절차를 수행한다. 또한, 클라이언트 시스템은 여러 개의 패킷 생성기로부터의 메시지 큐의 타입에 따라 다중 패킷 생성기를 지원할 수 있도록 구현되었다.



(그림 12) 사용자 데이터 보안 시뮬레이터 구성

패킷 생성기는 시작 옵션의 호스트 시스템 이름, 포트 번호와 사용자 터미널로부터 또는 파일로부터 입력된 데이터를 이용하여 20바이트의 TCP헤드(send_tcp), 20바이트의 IP 헤드(send_ip) 정보를 생성하고 사용자 데이터를 구성한다. 생성된 패킷은 UNIX운영체제에서 프로세스간 통신 방식인 메시지 큐 또는 다른 시스템에 시뮬레이터 클라이언트가 존재하는 경우 TCP/IP 소켓을 이용하여 전달한다. 클라이언트 및 서버 시스템은 패킷 생성기로부터 전달된 메시지 정보로부터 TCP/IP헤드정보로부터 IPOA의 일부 기능인 TCP/IP 주소와 ATM의 VPI/VCI 주소로 매핑을 위한 기능을 처리하고 사용자 데이터인 서비스 데이터 유니트(SDU)를 추출하여 전자서명을 한 후 분할기능에서 48바이트의 데이터에 대하여 무결성을 보장하기 위한 다양한 암호 알고리즘을 이용하여 암호화 한 후 5바이트의 셀 헤드를 추가하여 53바이트의 셀을 서버 시스템으로 소켓을 통하여 전달하는 기능을 처리한다.

5.3.1 암호 알고리즘

본 고에서는 데이터 암호화에 주로 이용되는 대칭키 알고리즘인 DES의 ECB(Electronic CodeBook) 모드, 국산 표준 암호 알고리즘인 SEED, RC5와 스트림 암호화 방식의 일부 기능을 제공하는 BlowFish의 CFB64(Cipher FeedBack 64bits)와 OFB64(Output FeedBack 64bits) 등과 스트림 암호화 방식의 RC4, SEAL알고리즘을 적용하였으며, 추가적인 알고리즘을 적용할 수 있도록 구현하였다.

5.3.2 시뮬레이션

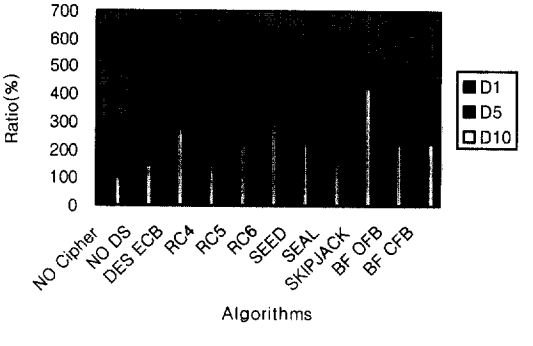
시뮬레이터를 이용하여 다양한 암호 알고리즘을 이용하여 ATM 네트워크에서 사용자 데이터 보안 과정을 시뮬레이션하고 그 결과를 산출, 분석하여 최적의 암호화 방식을 선택하여 국내에서 개발된 ATM 교환기의 최적의 보안 모델을 제시하고자 한다. 시험 방법은 전자서명시 대칭키 암호화방식에서 블록 암호 방식과 일부 스트림 암호 방식을 적용하여 성능을 분석하고, 데이터 암호화를 위하여서는 64비트 단위의 데이터 블록 암호 방식인 DES, RC5와 128비트 암호화 방식인 SEED, SkipJack, 그리고 가변 길이 데이터 암호화 기능을 제공하는 암호화 방식은 BlowFish CFB/OFB 방식과 스트림 암호화 방식인 RC4와 SEAL을 적용하여 성능을 평가한다.

5.3.3 시험 결과 및 분석

시험은 일정크기의 데이터를 생성하여 ATM 시뮬레이터에서 다음과 같은 경우로 시험을 한다. 시험 결과는 각 경우에 대하여 5번의 결과치의 평균값으로 평가하고 시험의 공정성을 기하기 위하여 한 대의 워크스테이션에서 한 사용자만 사용하여 외부적인 영향을 최소화 한다.

사용 워크스테이션은 SUN Microsystems사의 256MB의 주기억장치를 가진 UltraSparc-1를 이용하고, 암호 알고리즘은 openssl의 암호 알고리즘 라이브러리를 링크하여 사용한다. openssl에서 제공하지 않는 SEED와 스트림 암호 방식인 SEAL은 표준 라이브러리에 추가하였다.

시험 조건으로 사용자 데이터는 2M바이트의 ASCII 문자 데이터를 패킷 생성기를 이용하여 발생시켰다. 이 결과 암호화를 하는 경우 약 50%의 추가적인 셀 부하를 발생하였으며 암호 알고리즘에 따라 250%~600%의 전달 지연 현상을 발생하였다. 또한 공개키 방식인 RSA 알고리즘을 이용한 전자서명을 한 경우 약 100배의 전달 지연 현상을 나타내었다. TCP/IP 계층에서의 사용자 데이터 크기를 2M바이트로 하고 최대한의 외부적인 요소의 영향을 배제한 상태에서 시험한 결과, (그림 13)에서 보는 바와 같이 암호화를 하지 않은 상태에서의 ATM 적응 계층에서의 분할 및 재결합 기능 처리 성능에 비하여 데이터 암호화 기법을 적용하였을 경우 클라이언트 및 서버에서 스트림 암호화 방식인 RC4와 SEAL 알고리즘은 큰 차이는 없이 약 250% 내외의 성능 저하를 보였으며, 블록 암호화 방식 DES, BlowFish등에서는 350%~600%의 상당한 전달 지연 현상을 확인할 수 있었다. 결과적으로 전자서명



(그림 13) 시뮬레이션 결과

에 따른 부하가 ATM 셀을 생성하여 전달하는 과정에 비하여 상당한 프로세서의 부하를 유발하게 된다. 따라서, 통신 프로토콜에서 최적의 보안 기능과 최소한의 전달 지연을 위하여서는 암호화 및 복호화 기능을 전용 마이크로 프로세서에서 처리하고 암호 키 협상 및 갱신 기능은 주 프로세서에서 실행되는 실시간 운영체제에서 실행하여야 한다.

6. 결 론

지금까지 ATM 워크 보안에 대한 일반적인 사항과 ATM Forum 보안 모델을 중심으로 ATM 보안에 대해서 개략적으로 정리하고, 초고속통신망 환경에서 서비스 이용자의 데이터 보호를 위한 한가지 방법으로 가입자 유형별 보안 모델을 중심으로 소개하고 시뮬레이터를 통하여 암호 알고리즘에 따른 데이터 전달 능력을 분석하였다.

ATM 보안 분야에서 다루어질 주요 사항은 WAN 서비스를 보호하는 것이 주목적으로 ATM PVC 서비스인 경우는 네트워크 관리 분야에서, SVC 서비스의 경우는 WAN 환경에서 폐쇄사용자 그룹(Closed User Group) 서비스를 제공하게 되는데, 이러한 서비스는 데이터 암호화를 기반으로 ATM 호 접근 제어 방식을 이용하여 시큐리티를 제공한다. 또한 ATM 서비스 거부 및 신호 변경 등의 위협에 대응하기 위해 ATM 제어평면에 대한 보호 방법과 ATM 라우팅 및 라우팅 정보 변경에 대응한 보호 방법이 연구되어져야 한다.

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 방안, 네트워크 무결성은 네트워크내에서 악의에 의한 물리적 기능적 변경에 대한 완벽한 대응과 네트워크내에서 전달되는 데이터뿐만 아니라 일시적으로 저장되는 데이터에 대해 보호를 제공해 주는 방법에 대한•연구가 포함된다.

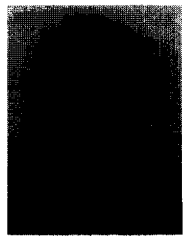
참 고 문 헌

[1] Peyravian and Van Herreweghen, "ATM Security Scope and Requirements," ATM Forum contributions 95-0579.

[2] ATM Forum, ATM Security Specification, ATM Forum/95-1473R3, August 1996.

[3] ATM Forum, ATM Security Framework Version1.0 ATM Forum/95-1473R5, ATM Forum/Security WG, October 1996.

[4] 강신각, "ATM 보안 기술 규격 분석", ETRI 내부문서 TDP TD96-5620-091, 1998.7.



장 종 현

e-mail : jangih@etri.re.kr

1988년 경북대학교 전자공학과 (공학사)

2000년 충남대학교 전자공학과 (공학석사)

현재 한국외국어대학교 전자공학과 박사과정

1988년~1994년 대우통신㈜ 종합연구소

1994년~현재 한국전자통신연구원 교환전송기술연구소 선임연구원

관심분야 : 네트워크 보안, 이동통신, 미들웨어 등

한 치 문

e-mail : cmhan@hyfs.ac.kr

1977년 경북대학교 전자공학과 (공학사)

1983년 연세대학교 대학원 전자공학과(공학석사)

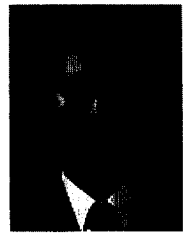
1990년 The University of Tokyo (동경대) 전자정보공학과 (공학박사)

1977년~1983년 한국과학기술연구원(KIST) 연구원

1983년~1997년 한국전자통신연구원(ETRI) 선연, 책연 교환기술연구단 계통연구부장 역임

1997년~현재 한국외국어대학교 전자공학과 교수

관심분야 : ATM 통신망 및 교환, IMT-2000 네트워크, 네트워크 보안 등



이 동 길

e-mail : dglee@etri.re.kr

1983년 경북대학교 전자공학과 (공학사)

1985년 한국과학기술원 전산학석사

1994년 한국과학기술원 전산학박사

1985년~현재 한국전자통신연구원 책임연구원

관심분야 : 컴파일러 구성론, 프로그램밍 언어론, 미들웨어 등