通信情報保護學會誌
第7卷 第1號, 1997. 3

초고속정보통신망을 위한 ATM 보안기술

ATM Security for Information Infrastructure

강 신 각*

요 약

ATM 기술에 기반을 둔 광대역통신망의 구축과 실용화가 추진되면서 기존의 인터넷이나 패켓망에서와 마찬가지로 ATM 망을 통해 전송되는 정보에 대한 보안 요구사항이 제기되게 되었고, 이 문제를 해결하기 위해 ATM 포럼에서는 보안 작업그룹을 설립하여 ATM 보안 규격 개발작업을 수행하고 있다. 본 고에서는 현재 ATM 포럼에서 추진되고 있는 ATM 보안규격 개발작업의 현황과 지금까지 연구 개발된 ATM 보안 규격의 주요 내용을 소개한다.

1. 개 요

컴퓨터와 통신 기술의 발전과 함께 다양한 멀티미디어 응용 서비스가 출현하면서 통신망의 고속화 및 광대역화가 요구되게 되었고, 이러한 요구사항을 효율적으로 만족시켜 줄 수 있는 새로운 통신 프로토콜 핵심기술로 ATM (Asynchronous Transfer Mode) 기술이 개발되었다. ATM 프로토콜은 광대역종합정보통신망 (B-ISDN) 구축의 핵심기술로 이용되고 있으며, 최근 세계적으로 활발하게 논의되고 있는 초고속 정보통신 기반구축을 위한 핵심기술로 연구되고 있다. 초기에 ATM 기술의 표준화 작업은 ITU-T를 중심으로 추진되어 왔으나 ATM 기술의 신속한 개발 및 상업화를 목적으로 산업체를 중심으로 한 ATM 포럼이 설립되면서 ATM 기술의 개발 및 보급이 더욱 활성화 되고 있고, 그 결과 ATM 기술을 채택한 제품이 이용자 들에게 공급되고 있으며 소규모 망이 구축되고 있다.

ATM 기술에 기반을 둔 광대역통신망의 구축과 실용화가 추진되면서 기존의 인터넷이나 패켓망에서와 마찬가지로 ATM 망을 통해 전송되는 정보에 대한 보안 요구사항이 제기되게 되었고, 이 문제를 해결하기 위해 ATM 포럼에서는 보안 작업그룹을 설립하여 ATM 보안 규격 개발작업을 수행하고 있다. 본 고에서는 현재 ATM 포럼에서 추진되고 있는 ATM 보안규격 개발작업의 현황과 지금까지 연구 개발된 ATM 보안 규격의 주요 내용을 소개한다.

* 한국전자통신연구소 정보통신표준연구센터

ATM 통신망에서의 보안 요구사항이 제기되면서 ATM 포럼에서는 1995년 6월에 Security Ad Hoc 그룹을 정식으로 설립하였다. Security Ad Hoc 그룹은 다시 1995년 12월에 독립적인 작업반으로 바뀌어 현재의 보안 작업반(Security Working Group)으로 개편되었고 현재는 이 보안 작업반을 통해 ATM 보안규격 개발작업이 진행되고 있다.

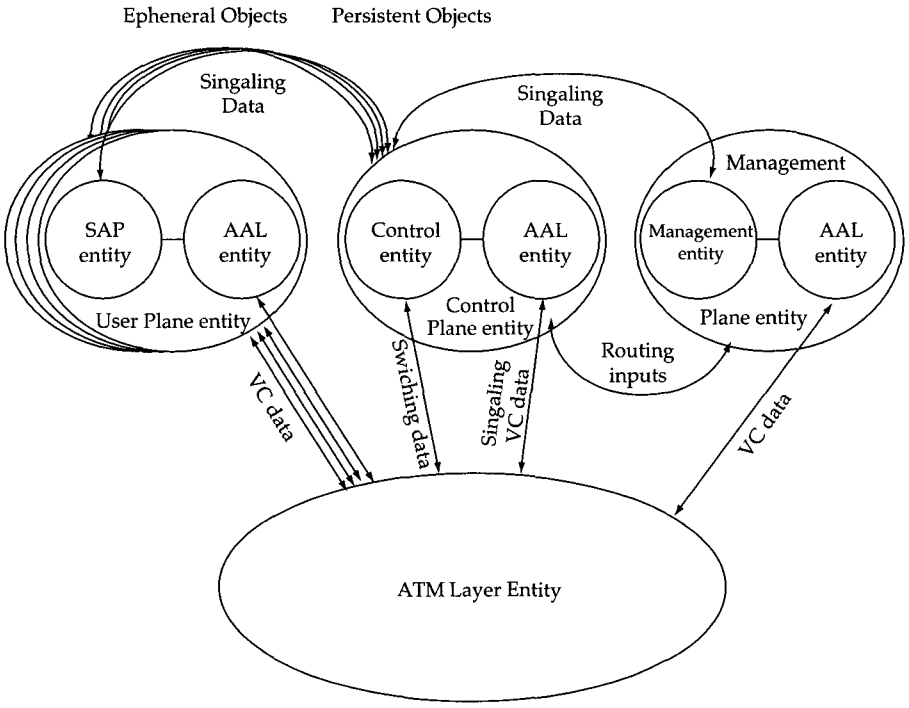
보안 작업반의 활동 목표는 ATM 보안을 위해 요구되는 요구사항을 연구하여 사용자 망간(UNI) 또는 망간(NNI) 접속부에서 암호학적으로 안전한 프로토콜과 알고리즘을 정의하고 이를 바탕으로 한 ATM 보안규격을 개발하는 것을 목표로 하고 있다. 그리고, 이러한 작업은 현재 ATM 표준에서 정의하고 있는 사용자평면, 제어평면, 그리고 관리평면 모두에 대한 보호 기능을 제공할 수 있는 ATM 보안규격 개발을 목표로 하며, 또한 이 규격에 따르는 보안 제품간 상호운용성 확보 방안을 포함하고 있다.

보안 작업반의 작업계획을 살펴보면, 먼저 ATM 보안규격 개발범위가 광범위한 점을 고려하여 규격개발 작업을 단계적으로 추진키로 하고 이를 제1단계와 제2단계로 분리하였다. 그리고 각 단계마다 규격개발 범위를 정한 다음 각 규격개발 대상에 대한 세부 요구사항을 정의하고, 다음 단계로 이러한 요구사항을 지원할 수 있는 메카니즘을 정의하여 규격을 개발한다는 전략으로 규격 개발 작업을 추진하고 있다. 제1단계 규격 개발작업은 '97년 2월까지 최종 투표를 위한 보안규격 개발을 완료한다는 일정으로 작업을 진행하고 있다.

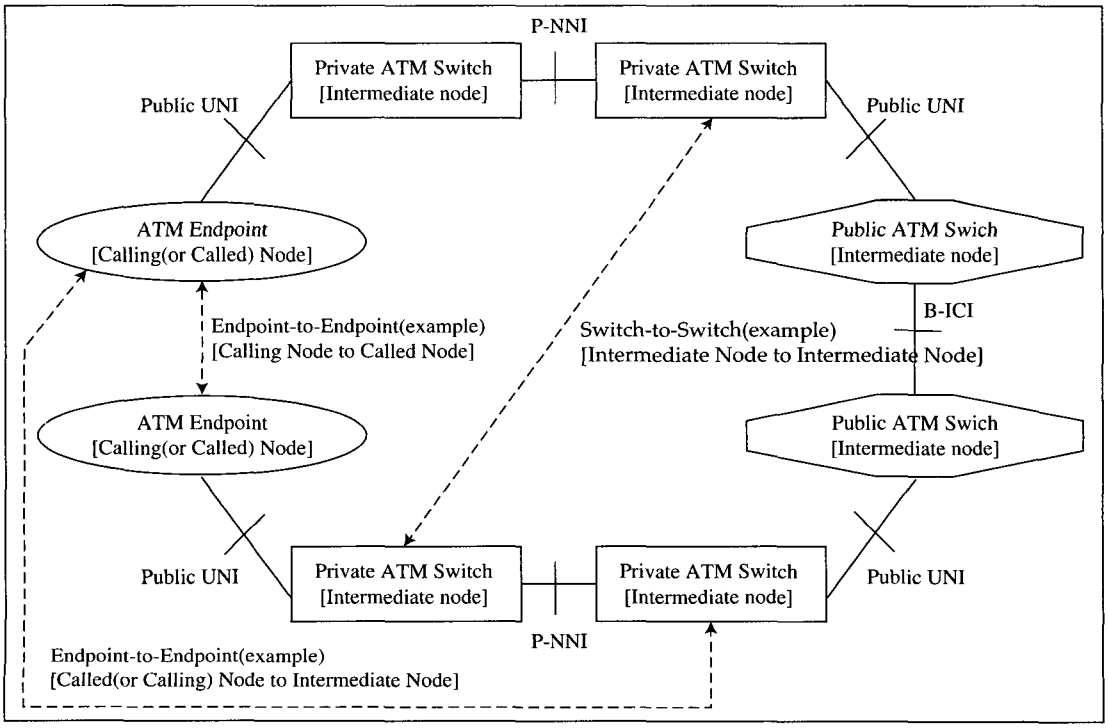
현재 ATM포럼에서 추진되고 있는 ATM 보안규격 개발 작업의 기본 방향을 살펴보면, ATM 기술을 사용하는 국가나 이용자들의 다양한 보안 요구사항을 지원할 수 있도록 복수의 암호 알고리즘과 서로 다른 암호키 길이를 지원하며, 제품개발자 고유의 확장은 허용하되 제품간 상호운용성을 확보하기 위해 필수적으로 사용되어야 할 보안 메카니즘을 정의한다. 그리고 보안 기능을 구현하지 않은 기존 ATM 장비와 호환성을 갖도록 하며, 보안 기능의 추가로 인한 다른 관련 규격에 끼치는 영향을 최소화 하도록 하고 있다. 이밖에도 향후 개발될 보안규격이 현재 개발되고 있는 보안규격과 호환성이 유지되도록 추진하며, 개발되는 보안 메카니즘은 대규모 사용자 수를 수용할 수 있도록 하고 있다. 특히 중요한 작업 방향 중 하나는 인증과 기밀성 메카니즘을 서로 분리시킨다는 것이다. 이는 기밀성 서비스가 각 국가나 기관의 특성에 따라 제한되는 경우가 많기 때문에 인증서비스와 기밀성 서비스를 위한 메카니즘을 서로 구별하는 것이 적절하다는 이유에서이다.

2. ATM 보안모델과 보안규격 범위

ATM 보안 규격의 범위와 요구되는 기능을 효율적으로 규정하기 위해 두 가지 참조모델을 정의하고 있는데, 하나는 단일 ATM 망 요소들 사이의 관계를 표시하는 객체모델이고 다른 하나는 ATM 망 요소들 사이의 접속부 및 상호동작 관계를 보여주는 접속부 모델이다. (그림 1)은 객체모델로 ATM 프로토콜 참조모델에 근거하고 있다. 이 모델을 통해 ATM 프로토콜에서 정의되고 있는 서로 다른 프로토콜 평면과 각 객체요소에 대해 임의의 보안기능을 규정해야 함을 알 수 있다. 또한 (그림 2)는 ATM 접속부 모델로 이 모델을 통해 종단간(Endpoint-to-Endpoint), 스위치간(Switch-to-Switch), 종단-스위치간(Endpoint-to-Switch) 등과 같은 다양한 상호접속 시나리오에 대해 보안기능을 규정해야 함을 알 수 있다.



(그림 1) ATM 망 객체 모델



(그림 2) ATM 망 접속부 및 상호 동작 모델

현재 개발되고 있는 ATM 보안규격은 사용자평면과 제어평면, 그리고 관리평면에 대해 요구되는 보안기능을 제공하기 위한 메카니즘을 정의하고 있으며, 종단간, 스위치간, 종단-스위치간 상호접속 시나리오에 대한 보안기능을 정의하고 있다. ATM 보안규격 개발작업은 제1단계와 2단계로 구분하여 단계적으로 추진되고 있는데 현재 개발중인 제1단계 ATM 보안규격의 범위는 다음과 같다. 먼저 사용자평면에 대해서는 가상회선(Virtual Circuit)에 대해 보안서비스를 적용하는 것으로 하고 있는데, 여기서 가상회선은 가상채널연결(VCC)이나 가상경로연결(VPC)이 될 수 있다. 사용자평면을 위해 정의되는 보안 서비스로는 접근제어, 인증, 데이타 기밀성, 데이타 무결성 서비스가 있다. 제어평면에 대해서는 강한 신호 메세지 인증 기능이 규정되어 있다. 즉, ATM 제어평면의 통신 실체는 연결 요청에 대해 자원을 할당하기 전에 신호 메세지의 발신자와 내용을 검사함으로써 망에서 발생할 수 있는 여러 형태의 공격에 대응할 수 있다. 그리고 지원기능으로써 공개키 확인 서비스를 위한 확인(Certification) 기반구조와 암호키 교환, 세션키 갱신, 그리고 보안서비스 선택사항 들에 대한 협상기능 등을 정의하고 있다.

제2단계 보안 규격에서는 제1단계에서 다루어지지 않은 나머지 보안 기능을 제공하는 것을 규격 범위로 다룰 예정이다. 현재 예상되는 2단계 작업 내용으로는 제어평면에 대해 메세지 기밀성 서비스, 그리고 관리평면에 대한 보안 서비스를 작업범위로 하고 있으며, 세부 작업대상에 대해서는 추후 2단계 규격개발 작업이 추진될 때 다시 정의될 것으로 보인다.

3. 사용자 평면에서의 보안 서비스

사용자 평면에서 제공되는 보안 서비스로는 먼저 인증과 데이타 기밀성, 그리고 데이타 무결성 서비스가 있다. 또한 지원 서비스인 암호키 교환과 인증 기반구조, 그리고 보안 서비스 선택기능 및 능력에 대한 협상 기능이 고려된다. 이러한 사용자 평면에서의 보안 서비스를 제공하기 위해서는 통신 실체간에 인증 메카니즘이나 데이타 기밀성 및 무결성 서비스를 위한 암호키 교환 메카니즘 등이 요구된다. ATM 보안 규격에서는 이를 위해 양방향(Two-Way)과 세방향(Three-Way) 보안 메세지 교환 프로토콜을 정의하고 있으며, 이 메세지 교환 프로토콜을 이용하여 인증, 무결성, 기밀성, 접근제어 서비스 등을 제공한다.

3.1 보안 메세지 교환 프로토콜

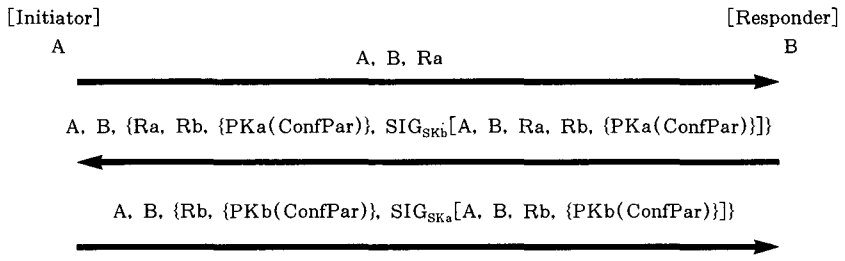
보안 메세지 교환 프로토콜은 사용되는 특정 암호 알고리즘과는 무관하며, 비대칭형(공개키) 인증을 위해서는 ISO/IEC 9594-8에 규정된 강한 인증 절차에 근거하여, 그리고 대칭형(비밀키) 인증을 위해서는 ISO/IEC 11770-2에 정의된 절차에 근거하여 정의된다. 여기서 정의되고 있는 보안 메세지 교환 프로토콜은 상호인증 기능과 일방향 또는 양방향 키 교환 기능을 제공한다. 세 방향 프로토콜의 경우 보안 서비스 및 선택사항들에 대한 기본 협상기능을 부가적으로 지원한다. 보안 메세지 교환 프로토콜을 기술하기 위해 사용되는 주요 표기법은 다음과 같다.

- PK_X : X의 공개키

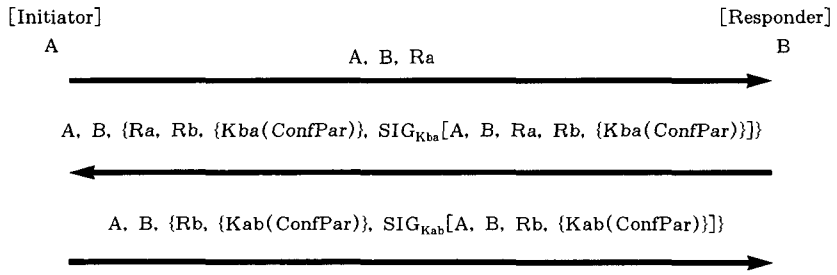
- SK_X : X의 비밀키
- PK_X(text) : text를 PK_X로 암호화
- SK_X(text) : text를 SK_X로 복호화
- K_{XY} : X, Y의 공유 비밀키
- K_{XY}(text) : text를 K_{XY}로 암호화
- SIG_{SK_X}[text] : text를 SK_X로 서명
- $SIGK_{xy}$[text] : text를 K_{xy}로 서명
- R_X : X가 생성하는 난수
- T_X : X가 생성하는 Timestamp
- H(text) : text의 일방향 해쉬

비대칭 암호 알고리즘에 근거한 세 방향 보안 메세지 교환 프로토콜의 흐름도는 (그림 3)과 같고, 대칭 암호 알고리즘에 근거한 세방향 보안 메세지 교환 프로토콜의 흐름도는 (그림 4)와 같다. 여기서 ConfPar 매개변수는 메세지 교환 프로토콜이 키 교환 메카니즘으로 사용될 때 교환될 암호키를 전송하는 영역으로 사용될 수 있다.

보안 메세지 교환 프로토콜은 실제ATM 환경에서 신호 프로토콜을 사용하여 동작하도록 할 수 있다. 즉, 보안 메세지를 기존 신호 프로토콜에 맵핑시켜 신호 프로토콜에 실어 전송함으로써 보안 메세지 교환 프로토콜이 동작되도록 하는 것이 가능하다. 또 다른 방법으로는 기존 신호 프로토콜에 아무런 변경을 가하지 않고 일단 사용자 연결이 성공적으로 확립된 이후에 보안 대리자(Security Agent)가 사용자 트래픽 채널을 통해 보안 메세지를 인-밴드로 전달함으로써 보안 메세지 교환 프로토콜이 동작되도록 할 수 있다. 인-밴드로 보안 메세지를 교환하는 방법은 보안 메세지 교환을 위한 중간 단계의 해결책으로 사용되기에 적합하다.



(그림 3) 비대칭 암호 알고리즘에 근거한 세방향 보안 메세지 교환 프로토콜



(그림 4) 대칭 암호 알고리즘에 근거한 세방향 보안 메세지 교환 프로토콜

3.2 인증과 암호키 교환 서비스

인증 서비스는 호출측과 피호출측 ATM 실체가 서로를 정당한 통신 상대인지를 식별하는 서비스로, 호출측과 피호출측 사이에 안전한 통신 채널을 확립하기 위해 요구되는 첫번째 필수 기능이다. 인증 메카니즘은 호출측과 피호출측 사이에 암호키의 안전한 교환과 보안 협상 매개변수의 안전한 교환 등과 같은 인증 서비스 외 다른 보안 서비스를 제공하기 위한 지원 서비스로도 사용될 수 있다. 인증 서비스는 대칭키 암호 알고리즘과 공개키 암호 알고리즘에 의해 실현될 수 있다.

인증 서비스는 앞에서 설명한 보안 메세지 교환 프로토콜에 의해 이루어 지는데 ATM 인증 서비스에 대한 주요 요구사항은 다음과 같다.

- 단방향(Unilateral) 인증과 상호(Mutual) 인증 선택 기능 제공
- 재연 공격을 막을 수 있어야 함
- 기존 신호채널을 사용하는 ATM 인증의 경우 단방향 인증은 한 개의 신호 메세지에 의해, 그리고 상호 인증은 두 개의 신호 메세지에 의해 이루어 짐
- 기본형 ATM 인증 기반구조는 대칭형 알고리즘에 근거해야 하며, 대칭형 알고리즘 기반 인증구조를 선택할 수 있는 협상기능을 제공하여야 함
- 적합한 구현은 기본형 암호 알고리즘들을 구현하여야 함
- 종단간, 그리고 스위치간 인증기능을 지원하여야 함

인증 서비스를 제공하기 위해 사용될 수 있는 암호 알고리즘들은 다음과 같다. 먼저 비대칭키(공개키) 방식을 사용할 경우에는 RSA, DSA, Elliptic Curve/DSA, ESIGN 암호 알고리즘 중 하나를 사용자 평면 인증을 위해 사용하여야 한다. 그리고 대칭키(비밀키) 방식을 사용할 경우에는 DES(CBC 모드)와 FEAL(CBC 모드) 중 하나를 사용자 평면 인증을 위해 사용하여야 한다.

암호키 교환은 인증 절차의 수행을 통해 동시에 이루어 질 수 있는데 비대칭키(공개키) 방식을 사용할 경우에는 RSA, Diffie-Hellman, Elliptic Curve/Diffie-Hellman 암호 알고리즘 중 하나를 사용하여야 한다. 그리고 대칭키(비밀키) 방식을 사용할 경우에는 DES(CBC 모드)와 FEAL(CBC 모드) 중 하나를 암호키 교환을 위해 사용하여야 한다. 또한 인증을 위해 해쉬 함수가 요구될 때는 SHA와 MD5 중 하나가 사용되어야 한다.

3.3 데이타 기밀성 서비스

데이타 기밀성 서비스는 ATM 연결을 통해 전송되는 사용자 데이타가 비 인가된 자에게로 유출되는 것을 막기 위한 암호학적 보안 메카니즘을 제공하며, 사용자 평면에서의 기밀성 서비스는 종단간, 그리고 스위치간 접속 시나리오에 대해 정의된다. ATM 계층과 AAL 계층에서 기밀성 서비스가 제공 가능하나 공통적인 기밀성 서비스 골격을 제공하기 위해 ATM 계층에서 기밀성 보안 서비스를 지원하도록 하고 있다. ATM 셀은 고정된 길이를 가지므로 DES, IDEA, CDMF, FEAL과 같은 대칭키 암호 알고리즘을 사용하기에 적합하다. ATM 사용자 평면에서의 기밀성 서비스를 위한 주요 요구사항은 다음과 같다.

- ATM 망의 중간 노드가 보안 서비스를 지원하지 않는다 해도 종단간, 그리고 스위치간 데이타 기밀성 서비스가 지원되어야 함.

- 데이타 기밀성 서비스는 ATM 셀 레벨에서 지원되어야 함.
- ATM 셀 헤더는 암호화되거나 변경되지 않아야 함.
- 상호운용성 확보를 위해 기본형 암호 알고리즘이 정의되어야 하며, 개발자에 따라 확장 및 선택기능을 허용해야 함.
- 키 갱신 동기화(key update synchronization) 메카니즘을 지원해야 함.
- 기본적인 선택사항 협상 메카니즘을 지원해야 함.

사용자 평면에서의 데이타 기밀성 서비스를 제공하기 위해 사용될 수 있는 암호 알고리즘으로 DES, Triple DES, 그리고 FEAL이 현재 ATM 보안규격에 정의되어 있다. 그리고 이들 알고리즘 중 하나가 사용될 때 ECB(Electronic Code Book) 모드, CBC(Cipher Block Chaining) 모드, Counter 모드 등이 기밀성 서비스를 위해 사용될 수 있다.

3.4 데이타 무결성 서비스

데이타 무결성 서비스는 사용자 데이타의 변경 등을 탐지할 수 있는 기능으로 AAL 3/4 및 AAL 5에 대해 AAL-SDU 레벨에서의 데이타 무결성 서비스를 지원한다. 또한 재연/재순서화(Replay/Reordering) 보호기능이 없는 무결성 서비스와 재연/재순서화 보호기능이 있는 무결성 서비스를 지원하며, 이러한 선택기능은 연결설정 단계에서 협상되어 선택된다. ATM 사용자 평면에서의 무결성 서비스를 위한 주요 요구사항은 다음과 같다.

- ATM 망의 중간 노드가 보안 서비스를 지원하지 않는다 해도 종단간 데이타 무결성 서비스가 지원되어야 함.
- 데이타 무결성 서비스는 AAL-SDU 레벨에서 지원되어야 함.
- 선택사항으로써 재연/재순서화 보호기능을 지원하여야 함.
- 상호운용성 확보를 위해 기본형 암호 알고리즘이 정의되어야 하며, 개발자에 따라 확장 및 선택기능을 허용해야 함.
- 키 갱신 동기화(key update synchronization) 메카니즘을 지원해야 함.
- 기본적인 선택사항 협상 메카니즘을 지원해야 함.

위 요구사항 중 데이타 무결성 서비스를 AAL-SDU 레벨에서 지원하는 이유는 전송 정보량이 지나치게 늘어나는 것을 막기 위함이다. 보통 데이타 무결성 서비스를 제공하기 위해서는 보호하고자 하는 단위 데이타 마다 8 바이트의 Timestamp와 8바이트의 메세지에 대한 서명값이 붙게 되며, 만일 48 바이트 길이를 갖는ATM 셀 데이타에 대해 무결성 서비스를 위한 추가 정보를 첨부한다면 17% ~ 33% 정도의 전송 오버헤드를 가져오게 된다. 따라서 AAL-SDU 단위로 무결성 서비스를 지원하는 것이 효율적이다.

선택사항으로써 정의되어 있는 재연/재순서화 보호 기능을 갖도록 무결성 서비스가 선택되면, 재연/재순서화 공격으로 부터 데이타를 보호하기 위해 AAL-SDU의 마지막에 먼저 6 바이트의 순서번호를 붙인 다음 전체 데이타에 대해 메세지 서명값을 계산하여 이 값을 전송함으로써 재연/재순서화 공격 여부를 탐지하게 된다. 현재 ATM 보안규격에서 정의하고 있는 암호 알고리즘에는 RFC 1828에 규정

되어 있는 Keyed MD5 방식과 ISO/IEC 9797에 규정된 블럭 암호화/CBC 방식이 있다.

3.5 접근제어 서비스

ATM 접근제어는 ATM-연결 서비스와 자산들에 대한 접근을 허용할 것인지를 규정하는 서비스로써, 실제 접근제어 기능은 구현 제품에 따라 서로 다르다 해도 제품간 상호운용성을 달성하기 위해서 접근제어 기능의 실현을 위해 요구되는 정보는 표준화 될 필요가 있다. 접근제어는 서비스 요청에 대한 규칙 집합이라고 할 수 있으며, ATM과 같은 접속지향형 서비스에서 CONNECT 서비스 프리미티브는 접근제어 서비스를 실현하기에 가장 적합한 요소가 된다. 접근제어 서비스를 적용하는 경우 임의의 규칙을 만족하면 요청하는 서비스가 제공되지만 규칙을 만족하지 못하는 경우에는 요청된 서비스가 거부되게 된다.

실질적으로 ATM 망에서 접근제어를 제공하는 방법에는 종단 사용자에 의한 방법과 관리기능에 의한 방법이 있다. 종단 사용자에 의한 접근제어는 사용자가 접근제어 서비스를 위한 규칙을 정의하는 형태로, 한 호스트가 ATM 연결을 확립할 수 있는 다른 호스트 목록을 제공하는 경우가 예가 될 수 있다. 관리기능에 의한 접근제어는 보통 집중형으로 접근제어가 이루어지게 되는데 예를 들면, 스위치가 ATM 연결이 허용될 수 있는 목록을 가지고 신호 프로토콜 동작시에 이를 제어함으로써 접근제어 서비스를 제공할 수 있다. 이때 스위치에 있는 접근제어 목록은 인가된 망 관리자에 의해서만 변경될 수 있게 될 것이다.

접근제어 서비스는 다양한 메카니즘에 의해 제공될 수 있으나 현재 ATM 보안 규격에서는 레이블 기반 접근제어를 정의하고 있다. 레이블 기반 접근제어 메카니즘은 민감도 수준(Sensitivity level) 개념에 근거하고 있는 방식으로 민감도 수준은 데이타의 노출에 대한 민감도를 나타낸다. 접근제어 서비스를 위한 주요 요구사항은 다음과 같다.

- ATM 접근제어 메카니즘은 연결 확립에 대해 사용자가 규정하는 접근제어와 장비 생산자 및 망 제공자가 규정하는 접근제어 기능을 지원해야 함.
- 접근제어 메카니즘은 사용자가 정의하는 접근제어 속성들을 오류없이 전달할 수 있는 선택기능을 가져야 함.
- 신호 프로토콜은 연결 설정 신호 메세지에 보안 레이블을 명시할 수 있는 능력을 제공하여야 함.
- 기본형 보안 레이블링 형식은 CIPSO 양식이 되어야 함.
- ATM 망관리 프로토콜은 각 ATM 물리 인테페이스에 대해 최대, 그리고 최소 보안 레이블을 명시할 수 있는 능력을 제공하여야 함.
- 다른 접근제어 알고리즘이 사용될 수 있도록 다른 레이블링 양식 규격을 허용하도록 해야 함.
- 복수의 접근제어 알고리즘이 동시에 사용되는 것을 허용하여야 함.

ATM 보안 규격에서는 현재 기본형 레이블링 양식인 CIPSO(Common IP Security Option) 양식에 대해 자세히 규정하고 있으며, 특정 보안 속성을 정의하는 CIPSO Tag 구조를 Tag Type 1, Type 2, 그리고 Type 5에 대해 명시하고 있다.

4. 제어 평면에서의 보안 서비스

제어 평면에서의 보안 서비스로는 현재 인증 서비스 만이 정의되어 있다. 제어평면에서의 인증 서비스는 ATM 신호 메세지를 신호 메세지의 발신자와 결합시키는 ATM 보안 서비스이다. 즉, 메세지 수신자나 제3자는 신호 메세지가 특정 발신자로부터 유래되었음을 확실하게 검증할 수 있도록 해 준다. 이러한 기능은 서비스 부인 공격으로 부터 보호할 수 있도록 해주며, 과금 등을 위한 감사정보에 대해 부인봉쇄 서비스를 제공할 수 있다. 또한 인증 메카니즘에 따라서는 종단간 데이타 무결성 서비스가 아울러 제공될 수 있다. 그렇지만 신호 메세지는 종단간 뿐만 아니라 hop-by-hop 중요성을 가진다는 측면에서 제어 평면에서의 인증은 사용자 평면에서의 인증과는 다른 특성이 있다. 즉, hop-by-hop 중요성을 가지는 신호 메세지의 경우에는 중간에 있는 ATM 스위치가 이 신호 메세지를 필요에 따라 다양한 처리를 하여야 하므로 적절한 인증 메카니즘을 사용하지 않는다면 종단간 메세지 무결성은 동시에 보장될 수 없다. 제어 평면에서의 인증 서비스를 위한 주요 요구사항은 다음과 같다.

- ATM 제어평면 인증 기반구조는 이미 인증된 메세지의 재연 공격으로부터 보호기능을 제공하여야 함.
- 인증 기반구조는 서비스 특정 매개변수들을 메세지 내에 포함하는 것을 허용해야 함. (서비스 특정 매개변수는 알고리즘 식별자, 키 길이, 공개 매개변수 등.)
- 기본형 인증 메카니즘은 비대칭키(공개키) 알고리즘 기반이어야 함.
- 인증 기반구조는 ATM 중간 노드가 보안 서비스를 지원하지 않는다 해도 종단간, 스위치간, 그리고 종단-스위치간 인증 서비스를 지원하여야 함.
- 비 인증된 메세지가 수신되면 요청되는 서비스는 거절되어야 하고 적절한 오류 보고가 수행되어야 함.
- 메세지를 검사하는 어떤 장치에 의해 인증 정보가 신호 메세지에 첨부되는 것이 허용되어야 함.
- 종단간, 그리고 hop-by-hop 인증 및 무결성 서비스가 지원되어야 함.

ATM 보안 규격에서는 제어 평면에서의 인증 서비스를 제공하기 위한 인증 정보 요소 형식을 정의하고 있으며, 추후 종단간, 스위치간, 그리고 종단-스위치간 시나리오 각각에 대해 인증 서비스를 규정할 예정이다.

5. 지원 서비스

ATM 보안 규격에서는 공개키 방식 암호 알고리즘을 기본적으로 사용하고 있으므로 공개키에 대한 확인기능이 필수적으로 요구되며, 통신 실체 사이에 안전하게 암호키를 교환할 수 있도록 하는 절차가 요구된다. 또한 일단 설정되어 사용되는 비밀 세션키를 계속해서 사용하는 것은 안전도에 문제가 있을 수 있기 때문에 비밀 세션키 자체를 주기적으로 혹은 필요에 따라 갱신하여 사용할 필요가 있으며, 이를 위해 비밀 세션키 갱신 절차 및 프로토콜이 요구된다. 이러한 서비스 들은 통신 실체 사이에 직접적인 보안 서비스를 제공하는 것은 아니지만 원하는 보안 서비스를 제공하기 위해서는 필수적으로 요구되는 지원 서비스 들이다.

5.1 공개키 확인(Certification) 기능

공개키 암호 시스템에서 사용되는 공개키의 소유자가 정당한 지를 확인하는 것은 공개키 암호 시스템의 적용을 위해 필수적으로 요구되는 사항이다. 이를 위해 공개키 확인기관(CA: Certification Authority)에서는 확인서(Certificate)라고 부르는 공개키 증명서를 발급하여 공개키에 대한 정당성을 확인해 주는 서비스를 제공한다.

확인서는 공개키 소유자의 이름, 공개키 정보, 그리고 기타 부가적인 정보로 구성되며, 신뢰할 수 있는 제3자 기관인 CA가 서명함으로써 생성된다. 일단 CA에 의해 서명된 확인서는 안전하지 않은 메세지 교환 수단을 통하여 전달될 수 있으며, 일반 사용자는 누구나 CA의 공개키를 이용하여 확인서를 복호화 해봄으로써 공개키의 소유자가 정당한지 여부를 검증할 수 있다. 공개키 확인과 관련된 주요 요구사항은 다음과 같다.

- 확인서는 수명주기가 끝난 이후에도 보존되어야 할 경우가 있으므로 명시적인 확인서 파기 방법이 제공되어야 함.
- 서로 다른 통신 영역이 상호 연결될 수 있고, 복수개의 인증기관이 존재할 수 있으므로 영역간 확인서의 발급과 파기 수단이 허용되어야 함.
- 계층적 확인(Hierarchical Certification) 모델과 교차 확인(Cross Certification) 모델이 허용되어야 함.
- 공개키 확인과 확인서 파기를 위한 기반 구조는 기본형 암호 알고리즘에 근거해야 하며, 이밖에 다른 암호 알고리즘을 지원할 수도 있어야 함.

현재 ATM 보안 규격에서는 ITU-T X.509 Version 3로 표준화된 확인서 양식을 채택하고 있다. X.509 Version 3 확인서는 버젼, 일련번호, 확인서 발급에 사용된 서명 알고리즘 식별자, 확인서를 발행하는 CA 식별자, 유효기간, 확인서의 주체(CA 또는 다른 실체), 그리고 확장자로써 확인서 형식(Certificate Type)과 확인 형식(Certification Type)으로 구성되며, 마지막에는 전체 정보에 대한 CA의 서명값이 온다. 확인서 형식은 확인서가 CA의 확인서인지 다른 종단 실체의 확인서 인지를 나타내며, 확인 형식은 확인서가 교차 확인 결과로 생성되는 것인지 계층 확인 결과로 생성되는 것인지를 나타낸다. 계층 확인과 교차 확인을 위한 CA의 구성 예를 보면 (그림 5)와 같다.

현재 ATM 보안 규격에서는 RSA와 MD5 암호 알고리즘을 이용하여 확인서에 대한 서명과 인증, 그리고 키 교환을 수행하는 것을 기본으로 채택하고 있다. 또한 인증서 교환 프로토콜(CEP: Certificate Exchange Protocol)을 네개의 CEP 메세지인 REQUEST, RESPONSE, CONFIRM-CEP, FAULT를 이용하여 인증서 교환 절차를 명시하고 있다.

5.2 키 교환 서비스

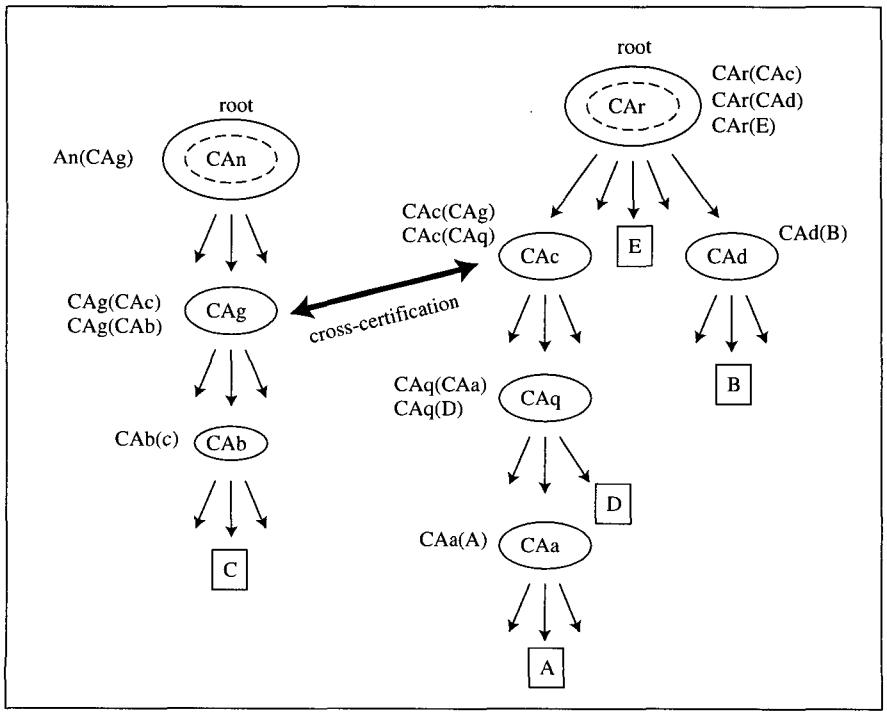
통신 실체간에 교환되는 정보를 암호화 하기 위해 사용될 비밀 세션키를 인증과 기밀성을 유지하면서 교환하는 절차는 보안 서비스를 제공하기 위해 필수적으로 요구되는 기능이다. 키 교환은 DES와 같은 대칭키 알고리즘에 의하거나 RSA와 같은 비대칭키 알고리즘에 의해 수행될 수 있다. 키 교환은 인증 메카니즘의 일부로 통합되어 인증과 키 교환이 동시에 수행 가능하며, 현재 ATM 보안 규격에

서는 이 방식을 제안하고 있다. 키 교환을 위한 주요 요구사항은 다음과 같다.

- 일방향과 양방향 키 교환 기능을 제공해야 함.
- 교환되는 키는 키 교환 당사자 외에는 알 수 없도록 기밀성이 유지되어야 함.
- 이미 사용된 키의 제연 공격을 막을 수 있어야 함.
- 기존 신호채널을 이용하여 키 교환을 하는 경우에는 일방향 키 교환은 단일 신호 메세지에 의해, 그리고 양방향 키 교환은 두 개의 신호 메세지를 이용하여 수행되어야 함.
- 기본형 키 교환 메카니즘은 비대칭키 알고리즘에 기반을 두어야 하나, 대칭키 알고리즘도 선택적으로 사용할 수 있도록 협상 기능을 제공하여야 함.
- 신호 채널을 이용한 키 교환 메세징 기능을 지원하여야 하며, 데이타 채널을 이용한 키 교환 메세징 기능도 부가적으로 지원되어야 함.

5.3 세션키 갱신 기능

데이타 기밀성이나 무결성 서비스를 제공하기 위해 사용되는 비밀 세션키의 수명 주기가 무한하지 않으므로 주기적으로 또는 필요할 때마다 갱신할 필요가 있으며, 일단 연결이 설정된 후 세션키를 갱신할 경우에는 완전한 인증 및 키 교환 프로토콜이 필요하지는 않다. 일반적으로 연결 설정시에 완전한 인증 및 키



(그림 5) 계층 확인과 교차 확인을 위한 CA의 구성 예

교환 프로토콜을 사용하여 마스터 키를 교환한 다음, 이 마스터 키를 사용하여 실제 응용 서비스 단계에서 사용될 세션키를 암호화 하여 전송함으로써 통신 상대간에 비밀 세션키를 공유하게 된다. 그리고 세션키 갱신 요구가 발생하면 세션키 갱신은 OAM(Operation and Maintenance) 셀을 이용하여 이루어지게 된다. ATM 계층에서 F4(가상경로 수준)와 F5(가상채널 수준)라는 두개의 OAM Flow가 정의되는데, 이들을 사용하여 세션키 갱신이 일어난다. 세션키 갱신 프로토콜은 개시자와 응답자간에 새로운 세션키 교환이 일어나는 세션키 교환(SKE: Session Key exchange) 과정과 사용되던 세션키로부터 교환된 새로운 세션키로 사용이 변경되는 세션키 변경(SKC: Session Key Changeover) 과정으로 이루어 진다. 먼저, 통신 상대 A, B간에 일어나는 세션키 교환 과정을 단계별로 보면 다음과 같다.

(1) A는 새로운 세션키 $K_{s,AB}$를 생성
(2) A는 키 번호 KN_A를 1 증가 시킴
(3) A는 세션키를 마스터 키로 다음과 같이 암호화
   - $EncK_{m,AB}(K_{s,AB}) = H(K_{m,AB}, B, KN_A, K_{m,AB}) \oplus K_{s,AB}$
(4) A는 KN_A와 $EncK_{m,AB}(K_{s,AB})$를 SKE OAM 셀로 B에 전송
(5) SKE OAM 셀을 수신하면 B는 KNA와 $EncK_{m,AB}(K_{s,AB})$를 추출한 후 다음 단계를 수행한다
   - KN_A가 A로 부터 수신되는 첫번째 세션키 이거나 최근 수신되었던 키 번호 보다 큰 값을 가지면 이것은 유효한 세션키가 되며
   - B는 다음과 같이 세션키를 찾아낸다.

$$K_{s,AB} = EncK_{m,AB}(K_{s,AB}) \oplus H(K_{m,AB}, B, KN_A, K_{m,AB})$$

SKE 과정을 통해 새로운 세션키가 교환되었어도 아직까지는 예전에 사용되던 세션키가 활성화 상태에 있으므로 새로운 세션키를 활성화 시키기 위해서는 세션키 변경 과정을 수행하여야 한다. 세션키가 일단 교환되면 A는 SKC OAM 셀을 B에게 보내 새로운 세션키를 사용할 것을 알린다. 이때 SKC OAM 셀은 수신측 B가 전환할 새로운 세션키 번호를 운반해 준다. SKC OAM 셀은 기밀정보를 포함하지 않으므로 암호화 되지 않고 평문으로 전송되며, 전송 오류를 고려해 SKC OAM 셀을 여러번 반복해서 보내게 된다. 수신측 B는 유효한 SKC OAM 셀을 수신하면 OAM 셀 수신 시점 부터 새로운 세션키를 사용하게 된다.

6. 결 론

최근 세계적으로 범 국가적 차원에서 적극적으로 추진되고 있는 초고속 정보기반 구축 노력의 주요 내용중 하나는 대용량 멀티미디어 정보가 통신망을 통해 막힘 없이 흐를 수 있도록 ATM 기술에 기반을 둔 고속 광대역 통신망을 구축하는 작업이다. 또한 이와 함께 중요하게 부각되고 있는 것이 바로 정보보호 요구사항이다. 본 고에서는 ATM 포럼을 중심으로 개발되고 있는 ATM 보안규격의 주요 내용과 최근의 작업현황을 소개하였다. 향후 초고속 정보기반이 성공적으로 구축되고 일반 사용자들이 이 초고속 정보기반을 통해 다양한 정보통신 서비스를 원활하게 이용할 수 있도록 하기 위해서는 정보보호 서비스가 필수적으로 제공되어야 할 것이다. 특히, 우리나라

의 경우 그동안 민간, 상업적인 분야에서 보안 기술에 대한 관심과 연구가 선진국에 비해 상대적으로 부족한 상황이었으며, 이로 인해 축적된 노하우 및 특허 등이 상당히 열악한 상황이다. 따라서 이제부터라도 보안 기술의 중요성을 인식하고 이에 대한 연구개발 노력이 더욱 적극적으로 이루어져야 할 것이다. 최근 정부에서 상업적인 목적으로 이용할 수 있는 정보보호 기술의 연구개발 및 기술 보급을 활성화 시키기 위하여 정보통신부 내에 정보보호과를 신설하고 정보통신부 산하 기관으로 한국정보보호센터를 설립하였으며, 각 연구기관 및 산업체에서도 정보보호 기술에 대한 관심 증대 및 연구개발 노력이 적극적으로 추진되고 있는 것은 시기적으로 적절한 일이다.

참 고 문 헌

[1] Thomas D. Tarman, Phase I ATM Security Specification(Draft), ATM Forum/95-1473R5, ATM Forum/Security WG, October 1996.

[2] 강신각, ATM에서의 보안기술, KRNET '96, 1996.

[3] ISO/IEC 9594-8, The Directory : Authentication Framework, ISO/IEC, 1995.

[4] ISO/IEC 9594-8/Amd.1, The Directory : Certificate Extensions, ISO/IEC, 1995.

[5] ITU-T Recommendation X.509, "The Directory : Authentication Framework, ITU-T, 1993.

[6] ISO/IEC 11770-2, Key Management - Mechanism using symmetric algorithm, ISO/IEC

[7] IETF Network Working Group, IP Authentication using Keyed MD5, RFC 1828, August 1995.

[8] IETF Network Working Group, The MD5 Message Digest Algorithm, RFC 1321, April 1992.

[9] IETF CIPSO Working Group, Common IP Security Option, Version 2.3, March 1993.

[10] ISO/IEC 9797, Data Integrity Mechanism using a Cryptographic Check Function Employing a Block Cipher Algorithm, 1994

□ 著者紹介

강 신 각

1984년 3월 충남대학교 전자공학과(학사)
1987년 7월 충남대학교 전자공학과(석사)
1984년 3월 - 현재 한국전자통신연구원 정보통신표준연구센타 책연

※ 관심분야 : 정보보호, 멀티미디어, 고속통신