ATM 망에서의 정보보호 구조 및 인증절차에 관한 연구

신 효 영† · 유 황 빈††

요 약

최근 ATM 망에서 제공되는 서비스가 다양해짐에 따라 통신정보의 보호에 대한 필요성도 높아지고 있는 실정이다. 그러나 ATM 망에 정보보호 기능을 추가하는 경우, 정보보호 위협 요소들을 분석한 후 기존의 ATM 망과의 호환성 및 투명성을 고려하여 설계하여야만 한다.

본 논문에서는 사용자 평면의 ATM 계층구조 내에서 정보보호를 담당할 정보보호프로토콜을 설계하고, 이 계층 내에서 필요한 프리미티브 및 메시지 처리절차들을 정의하였다. 또한 호 설정시 적용할 수 있는 인증 및 키 분배 프로토콜을 제시하였다. 제안된 인증 프로토콜은 점대점 방식뿐만 아니라 점대 다중 방식에서도 사용할 수 있다. GNY 로직을 통하여 인증 프로토콜의 정확성을 분석해본 결과, 인증 및 세션키 분배가 안전하게 이루어짐을 보여주었다.

A Study on the Security Structure and Authentication Procedure in ATM

Hyo-Young Shin† · Hwang-Bin Ryou††

ABSTRACT

Recently as services in ATM are diversified, the need for security has been increased. But when we added the security features in ATM, the compatibility and transparency with existing systems must be considered after analyzing threats of security.

This paper designs the security protocol in ATM protocol stack and defines the primitives and processing procedure of messages which are needed in the security layer. Also, this paper presents the authentication and key distribution procedure which can be adopted at call establishment. The presented authentication protocol can be used for point-to-point method as well as point-to-multipoint method. And the correctness of this protocol is verified using GNY logic.

1. 서 론

ATM 망이 보급되어 일반화됨에 따라 본격적인 멀티미디어 통신의 시대가 열리고 있다. 통신의 이용이 늘어나면서 기업이나 개인의 비밀 보호를 위한 요구 또한 높아지고 있는 실정이다. 다른 통신망과 같이 ATM 망도 도청과 비인가된 접근에 취약하다. ATM 망에서의 정보보호 위협요소는 비밀성, 무결성, 인증, 액세스 제어의 네 가지로 분류 할 수 있다[1]. 비밀성은 통신 내용의 도청을 방지하는 것이며, 암호화를 통

※ 이 논문은 1997년 광운대학교 교내 연구비 지원에 의해 연구되었음.
† 정 회 원 : 경북대학 사무자동화과 교수
†† 종신회원 : 광운대학교 컴퓨터과학과 교수
논문접수 : 1998년 3월 7일, 심사완료 : 1998년 12월 1일

하여 해결할 수 있다. 무결성은 정보를 변경한 시도를 발견해내는 것이며, 해쉬 함수를 이용한 전자서명을 이용하여 만족시킬 수 있다. 인증은 송, 수신자의 신분을 상호 검증하는 것이며, 이를 위해 인증 프로토콜을 사용한다. 액세스 제어는 보안정책의 정의와 구현을 통하여 자원의 접근을 제한하는 것이다.

ATM은 사용자 평면, 제어평면, 관리자 평면의 세 가지 평면으로 구성된다. 데이터의 비밀성 및 무결성 기능은 사용자의 데이터 전송을 담당하는 사용자 평면에서 고려될 수 있고, 인증 기능은 호 설정을 수행하는 제어 평면에서 다룰 수 있다. ATM에 적용할 수 있는 암호 방식에는 크게 비밀키 암호와 공개키 암호의 두 가지로 분류할 수 있다. 비밀키 암호는 암호화 키와 복호화 키가 같으며, 이 키를 송, 수신자가 공유하여 사용한다. 공개키 암호는 공개키를 알고 있는 누구라도 비밀통신의 송신자가 될 수 있는 점, 비밀키를 알고 있는 한 사람만이 서명할 수 있는 점에서 비밀키 방식보다 우수하지만, 계산량이 증가함에 따라 고속의 처리가 불리한 단점이 있다.

본 논문에서는 사용자 평면의 ATM 계층구조내에서 정보보호를 담당할 정보보호프로토콜을 설계하고, 이 계층내에서 필요한 프리미티브 및 메시지 처리절차들을 정의하였다. 또한 호 설정시 적용할 수 있는 인증 및 키 분배 프로토콜을 제시하였다. 본 논문에서는 비밀키 방식과 공개키 방식을 같이 사용하는 하이브리드 암호 방식을 적용하였다. 즉 대량의 데이터 전송시에는 속도가 빠른 비밀키 방식을 사용하고, 세션 키 분배 및 인증을 위해서는 공개 키 방식을 사용한다.

2. ATM 망을 위한 정보보호 구조

2.1 관련 연구

Stevenson[1] 등은 링크 레벨에 key agility 기능을 하드웨어로 구현하였으며, 손실된 셀을 단일한 암호 체인으로 한정시키기 위하여 동기 셀을 사용하였다. 이 방식은 링크 레벨에서 암호화가 수행되어 ATM LAN과 ATM WAN 사이에 보안 게이트웨이가 필요할 때 효과적일 수 있으나 스위치만을 보호하게되어 같은 스위치에 연결된 종단 시스템간의 공격이 가능한 단점이 있다.

Deng[2]의 연구에서 상호 시스템간의 인증, 보안 association의 설정, 암호키 분배와 같은 보안 관련 기능은 제어 면에서 수행되며, 사용자 트래픽의 보호는 사용자 면에 DPL(Data Protection Layer)을 정의함으로써 이루어진다. DPL은 AAL 계층의 CS와 SAR 사이에 위치하며, 제어 면에서의 자료전송은 DPL에 의해 보호되지 않는다. 이 방법은 time-stamp를 기반으로한 인증 프로토콜을 사용하여 동기화된 클럭이 유지되어야 한다.

Chuang[3]은 암호화 장치를 이용하여 ATM 계층에 비밀성 기능을 구현하였다. AAL5의 PDU 토큰을 이용하여 새로운 키와 초기화 벡터 등을 갱신하여 다음 블럭의 데이터를 암/복호화 하는데 이용하도록 하였다. 그러므로 키나 초기화 벡터가 변경되면, AAL 계층에서 ATM 계층으로 인터럽트가 발생하여 ATM 계층의 작업을 잠시 중단 시킨채 ATM 계층의 키와 초기화 벡터 변경 작업을 수행한다. 이 방법은 동기화를 시켜주는 계층과 암호화를 수행하는 계층이 다른 문제점이 있을뿐만 아니라 하위 계층이 상위 계층의 PDU 구조를 이해하고 있어야 하는 문제점이 있다.

2.2 제안구조

물리계층에 암호화 기능을 두는 경우, ATM 망으로 전송되는 모든 데이터들을 암호화하여 데이터 비밀성 뿐만 아니라 트래픽 비밀성을 제공할 수 있다. 이는 헤더를 포함한 전체 메시지를 암호화하기 때문에 중간 스위칭 노드들에서 라우팅을 위해 복호화가 필요하게 되며, 이 과정에서 메시지 수정, 삽입, 순서변경 등의 공격에 취약할 수 있다. 또한 전체 메시지를 암호화하므로써 암호화 과정을 채널의 속도와 정합시켜서 운영하는데 문제가 될 수 있다. 이러한 문제점들로 인하여 물리계층에 정보보호 기능을 두는 것은 적합하지 않다고 볼 수 있다.

ATM 계층에 암호화 기능을 두는 경우, 헤더 부분을 제외한 메시지를 암호화하게 됨으로 물리계층에서의 암호화보다 적은 비트율을 이용하게 된다. 그러나, ATM 계층은 헤더 정보가 생성되어 셀에 추가되는 곳이므로 암호화를 시키기 위해서는 부적절할 수 있다. 중간망의 노드들이 ATM 계층에서 셀 스위칭을 하므로 전체 망에서 암호 장비가 필요한 단점이 있다.

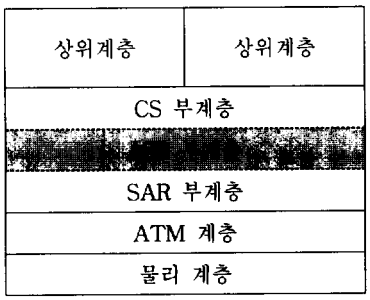
암호화 기능을 AAL 계층 이상에 두는 경우 보호 기능을 종단 사용자들에게까지 확장시킬 수 있으며, 하나의 ATM VC상에 멀티플렉스 되는 여러 세션들에 대해 각기 다른 보호 기능을 둘 수 있다. 그러나 이

방법은 하위 계층에 보호기능을 두는 경우보다 비용이 많이들 수 있다. AAL 계층의 상위계층에는 현재 여러 가지 전송 프로토콜과 응용프로그램들이 존재할 수 있으며, 이러한 모든 프로토콜 상에 보호 서비스를 구현해야 함을 의미한다.

AAL 계층은 프로토콜 스택상의 상위계층에서 요구되는 기능들을 지원하며, 서비스 사용자들의 요구를 충족시키기 위하여 AAL 형태 1, 2, 3/4, 5 등의 프로토콜을 지원한다. AAL 계층은 CS와 SAR 부계층으로 구성되며, AAL 계층에 암호화 기능을 부여하는 방안에는 CS 내, CS와 SAR 사이, SAR 내에 위치시키는 세 가지 방법이 있을 수 있다. 암호화 기능을 CS 내에 두는 경우에는 AAL 형태별로 필요한 요구사항들을 모두 고려해주어야 하므로 작업이 번거로워진다. SAR는 CS PDU를 48 바이트로 분할시키는 곳이며, 암호화로 인하여 데이터가 확장되는 경우의 처리가 어려워져 암호 알고리즘 선택에 대한 유연성이 줄어든다. CS와 SAR 사이에 두는 경우 암호화로 인하여 데이터가 확장되더라도 SAR로 데이터가 전송되기 이전이므로 확장으로 인한 영향을 받지 않으며, 정보보호와 관련된 추가의 기능들을 쉽게 구현 가능하다.

(1) ASP 부계층의 위치

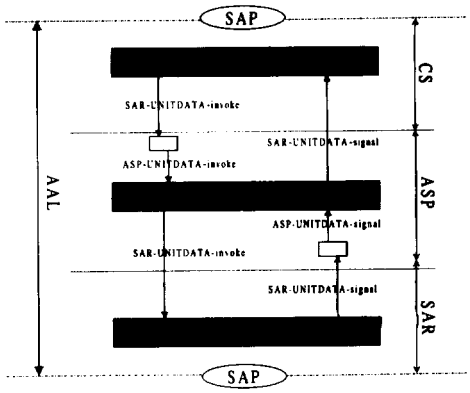
ASP(ATM Security Protocol) 부계층을 AAL 계층의 CS와 SAR 사이에 위치시킴으로써 다음과 같은 장점을 가질 수 있다. ASP 부계층은 CS와 SAR에 투명하게 동작한다. 이는 AAL 형태별로의 요구사항들을 고려할 필요가 없을 뿐만 아니라 상위계층의 응용프로그램별로 보호서비스를 개발할 필요가 없음을 의미한다. ASP 부계층은 SAR 부계층위에서 동작하기 때문에 암호화나 해쉬함수의 사용으로 인하여 데이터가 확장되더라도, 이를 SAR 부계층에서 분할/조립하므로 자연스럽게 처리될 수 있다. 이는 별도의 기능을 추가할 경우에도 구현이 용이해질 수 있다. ASP 부계층은 종단간의 암호화를 제공하므로써 전체 망에서의 암호화 장비를 필요치 않게 하고, 중간 노드들에서의 불필요한 암호화/복호화를 피할 수 있게 하여 이 과정에서의 공격 가능성을 방지할 수 있게 한다. 또한, 무결성 검사와 암호화를 같은 ASP 부계층에서 수행하므로써 키 분배 및 동기화 문제를 쉽게 해결할 수 있다. (그림 1)은 정보보호를 위한 ASP 부계층의 위치를 나타낸다.



(그림 1) ATM 정보보호 프로토콜 구조
(Fig. 1) The protocol stack for ATM security

(2) ASP 부계층을 위한 프리미티브

ASP 부계층을 위하여 기본적으로 ASP-UNITDATA-invoke, ASP-UNITDATA-signal 프리미티브가 필요하다. 부계층 사이에는 SAP가 존재하지 않기 때문에 이를 구분하기 위하여 request와 indication대신에 invoke와 signal을 사용한다. ASP 부계층은 CS PDU의 암호화와 메시지 인증을 위한 처리를 수행하고 기존의 SAR-UNITDATA-invoke와 SAR-UNITDATA-signal의 매개변수들을 SAR와 CS에 전달하여 주는 기능을 수행한다. 따라서, ASP-UNITDATA-invoke 와 ASP-UNITDATA-signal의 매개변수에는 기존의 SAR-UNITDATA-invoke와 SAR-UNITDATA-signal의 매개변수에 암호화와 메시지 인증에 필요한 매개변수들을 추가하였다. 프리미티브의 구체적인 내용과, 메시지 처리절차, 세션키 처리절차에 관한 구체적인 사항은 [6], [7]을 참고하기 바란다.



(그림 2) ASP 부계층을 위한 프리미티브
(Fig. 2) The primitives for ASP sublayer

3. 인증절차

ATM에의하여 접속되는 VC(Virtual Circuit)는 인증되지 않은채로 사용된다. VC의 한쪽 끝에 있는 사용자는 다른쪽 끝에 있는 사용자를 검증할 방법이 없다. 이로 인하여 종단 시스템이나 중간의 스위치들을 변조하여 자신의 신분을 쉽게 위장할 수 있다. 인증 기능을 VC 수준에서 제공하지 않고 상위의 응용계층 수준에서 제공할 수도 있다. 즉 망의 스위치에서 속임수가 발생하더라도 상위계층의 응용 프로그램에서 시스템 엔티티들을 인증 한다면 이를 발견할 수 있다. 그러나 이러한 속임수는 ATM의 접속이 설정된 후에 발견될 수 있기 때문에 효율성 면에서 좋지않다고 할 수 있다.

인터넷상에서는 사용자의 신원을 파악하기 위하여 IP 주소를 사용하는 경우가 있으나, 이는 외부의 라우터와 호스트들을 무조건 신뢰한다는 단점이 있다. 즉, IP 주소 자체에 대한 인증이 없기 때문에 망에서의 신원을 쉽게 위조할 수 있다. 또한 상위 계층의 모든 응용 프로그램이 안전하다고 기대하는 것은 비현실적이며, 보안 메커니즘을 모든 응용프로그램에 설치하거나 수정하는 것은 많은 시간과 비용이 소모될 뿐만 아니라, 중복된 작업이 필요하게된다.

VC별로 ATM 접속이 이루어질 때 인증 절차가 구현되면, VC가 접속이될 중간 스위치들에서의 속임수를 접속 완료 이전에 발견하는 효율성을 얻게된다. 또한 호 접속시 인증 작업이 선행됨으로써 상위 응용프로그램들마다 인증 절차를 구현하는 노력과 비용을 절감할 수 있게된다. 결론적으로 VC별로의 호 접속시 인증 절차는 매우 필요한 것이라 할 수 있다. 본 장에서는 ATM 호 접속 절차를 기술한 후 인증절차를 제시한다.

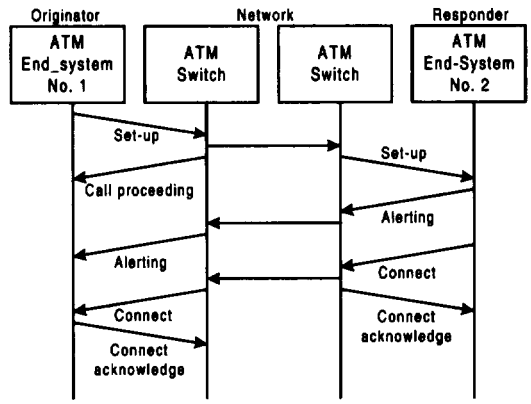
3.1 시그널링 시스템과 프로토콜

시그널링 시스템 No. 7에 대한 ITU-T 권고안은 Q.700 시리즈에 NNI 시그널링 시스템의 N-ISDN 버전을 포함하고 있다. N-ISDN에서 음성 표준에 대한 권고안은 Q.930, Q.931과 Q.93B에 정의되어 있다. B-ISDN을 위한 DSS(Digital Subscriber Signalling System) No. 2는 Q.2931의 최종본에 정의되어 있으며, Q.298x의 초안은 Q.93B와 Q.931을 기초로 하고 있다. ETSI (European Telecommunications Standard Institute)는 UNI 시그널링 프로토콜을 정의하는 중에 있다. ATM 포럼은 UNI 3.0을 정의하였으며, 현재 UNI 3.1로 수정중이다. 3.1은 이전 버젼과 호환성이 없으며, UNI 4.0을 위한 작업이 진행되고 있다.

3.2 시그널링 메시지와 절차

ATM망에서의 사용자 통신은 ATM 접속의 설정후에 일어난다. ATM 접속은 Set-up 요구 정보를 하나나 여러개의 목적지에 전송하는 시그널링 메시지에 기초를 두고 있다. 요구에 따라 망의ATM 스위치나 목적지의 ATM 종단 시스템은 메시지에 포함된 정보를 참조하여 처리를 한다. 호 접속시 적절한 VP의 선택, VCI와 VP를 중간 스위치에 연결, 스위치들간의 자원협상, 송, 수신 종단 시스템에서의 호 연결제어등과 같은 관리 작업을 수행한다.

Q.2931/Q.298x, UNI 3.0과 UNI 3.1은 호 접속을 수행하기 위한 절차와 메시지에 대한 사양을 포함하고 있으며, 점대점(point-to-point) 뿐만 아니라 점대 다중(point-to-multipoint) 연결에 관한 사양도 포함하고 있다. 이들 권고안내의 메시지는 시그널링 정보를 교환하기 위하여 사용되며, 메시지정보 요소 내에서 구체적인 내용을 제공한다. (그림 3)은 시그널링 메시지를 이용하여 호를 접속하는 과정을 나타내고 있으며, 이 과정에서 발신측과 착신측은 서로 다르게 동작한다.



(그림 3) 메시지를 이용한 ATM 호 접속의 예
(Fig. 3) An Example of ATM Connection Set-Up Using Messages

발신측은 처음에 "Set-Up" 메시지를 전송함으로써 호를 요구한다. 호가 받아들여질 수 있으면, "Call Pro-

ceeding" 메시지나 "Connect" 메시지 내에서 호를 시작시키는 ATM 종단 시스템 1에 대해 새로 할당할 수 있는 VPI/VCI를 결정하여야만 한다. 그렇지 않을 경우, 호의 발신측을 향하는 "Release Complete" 메시지를 통하여 망이나 ATM 종단 시스템 2가 접속할 수 없는 상태임을 알린다. 수신측은 시도된 호에 대한 "Set-Up" 메시지를 수신하여 입중계되는 호를 수락하면 "Alerting"과 "Connect" 메시지를 전송하고, 거부하기로 결정할 경우 "Release Complete" 메시지를 전송한다. 마지막으로 각 종단 시스템과 직접 연결된 스위치 사이에 "Connect Ack." 메시지가 교환된다. 점대다중 접속의 경우에는 "Add Party"와 "Add Party Ack." 메시지로 구성된다.

3.3 제안 인증 프로토콜

ATM 호 설정시의 인증은 점대점의 경우 "Set-Up", "Connect", "Connect Ack." 세 개의 메시지 내에서 이루어져야 하며, 점대 다중의 경우 "Add Party", "Add Party Ack." 두 개의 메시지 내에서 이루어져야 한다. 본 논문에서는 공개키 방식을 이용하여 양 사용자의 인증을 수행하면서 세션키의 분배를 수행하는 인증 프로토콜을 제시한다. 공개키 방식은 비밀키 방식에 비해 암, 복호화 속도가 느리므로 키분배 및 인증시에만 사용을 하고 데이터 전송시에는 속도가 빠른 비밀키 방식을 이용한다. 다음은 키 분배 및 인증 절차이다.

1. $A \rightarrow B : \{B, T_A, \{B, R_A, K_S\}_{SA}\}_{PB}$
2. $B \rightarrow A : \{A, T_B, \{A, R_A, R_B, K_S\}_{SB}\}_{PA}$
3. $A \rightarrow B : \{B, R_B\}_{PB}$

1. A는 세션키 K_S를 생성하여 B의 식별자, 타임 스탬프 T_A, 난수 R_A와 함께 B의 공개키 PB로 암호화하여 B에게 전송한다. 여기서 B, R_A, K_S는 A의 비밀키 SA로 암호화한 상태이다. 메시지의 내용이 B의 공개키로 암호화되었기 때문에 메시지는 B만이 복호화 할 수 있다. 또한 세션키 K_S는 A의 비밀키로 암호화되었기 때문에 B는 세션키를 A가 생성하여 보낸 것임을 확신할 수 있다. 타임 스탬프 T_A를 사용함으로써 재생 공격을 방지할 수 있다.
2. B는 A에게 세션키 K_S를 A의 식별자, 타임 스탬프 T_B, 난수 R_A, R_B와 함께 A의 공개키 PA로 암호화시켜 A에게 전송시킨다. 이 메시지에서도 A, R_B, K_S는 B의 비밀키 SB로 암호화된 상태로 전송된다. 메시지가 A의 공개키로 암호화되어 있기 때문에 A만이 수신하여 메시지의 내용을 복호화할 수 있다. K_S의 내용은 B의 비밀키로 암호화되어 있어서 A는 B로부터 전송된 메시지임을 확인할 수 있다. A는 난수 R_A를 통하여 자신이 전송했던 메시지임을 확신할 수 있다.
3. A는 B의 식별자와 R_B를 B로 전송한다. B는 R_B를 검사하여 자신이 전송했던 것과 일치하는 가를 확인한다.

점대점 방식의 접속에서는 세 개의 메시지가 사용되므로, 메시지 1, 2, 3을 통하여 인증 및 키분배를 수행할 수 있다. 그러나 점대 다중 방식의 접속에서는 두 개의 메시지만 사용되므로 위 절차중 1, 2 단계를 통하여 인증 절차가 수행되어야 한다. 위 절차의 단계 1, 2만을 적용하더라도 A, B 간의 인증과 키 분배가 안전하게 수행될 수 있는가를 검증해볼 필요가 있다.

3.4 제안 인증 프로토콜의 분석

4.3절의 인증 프로토콜을 검증하기 위하여 GNY 로직을 사용하였다. GNY 로직은 BAN 로직[5]을 기초로 하여 Li Gong, Roger Needham, Raphael Yahalom이 만든 검증 로직이다. GNY 로직은 BAN 로직과 같이 믿음을 바탕으로 한 추론을 기반으로 프로토콜을 단계적으로 분석하며, 이를 위해 요구되는 가정들을 명확하게 명세하고 최종적으로 얻는 결과로부터 결론을 내리는 방식을 택한다. GNY 로직은 BAN 로직에 비하여 다음과 같은 여러가지 장점을 가지고 있다.

- BAN 로직과 같이 여러 가지 일반적인 가정을 필요로 하지 않는다.
- 인식 규칙을 도입하여 수신자가 기대하는 메시지를 구분해주는 능력을 제공한다.
- 단순히 소유하는 것과 믿는 것을 구분함으로써 메시지의 내용과 메시지가 의미하는 것을 분리 가능하게 해준다.
- 발생처 개념을 도입하여 세션내의 특정한 메시지가 수신자 자신의 이전 메시지의 재생이 아님을 결정할 수 있도록 해 주었다.
- 경우에 따라 평문 메시지도 새로운 결론을 얻기 위하여 사용될 수 있다.

GNY 로직에 대한 구체적인 사양은 참고문헌 [4]를

참조하기 바라며, 여기서 로직에 대한 자세한 설명은 생략하였다. 다음은 인증 프로토콜 절차에 대한 정확성을 검증하기 위하여 GNY 로직으로 분석한 내용이다.

(1) 초기 조건 및 기본가정

프로토콜 수행 초기에 다음을 가정한다. 즉, A와 B는 서로의 공개키를 알고 있고, 자신의 비밀키를 소유한다. 또한 A, B 각각은 난수와 타임 스탬프를 생성하고, 세션키는 A에서 생성하며, 이의 중복성이 없음을 믿는다.

$A \ni PA,\quad A \ni SA,\quad A \ni PB$

$B \ni PB,\quad B \ni SB,\quad B \ni PA$

$A \ni T_A,\quad A \ni R_A\quad B \ni T_B,\quad B \ni R_B$

$A \mid\equiv \xrightarrow{+PA} A,\qquad A \mid\equiv \xrightarrow{+PB} B$

$B \mid\equiv \xrightarrow{+PB} B,\qquad B \mid\equiv \xrightarrow{+PA} A$

$A \mid\equiv \#(R_A),\quad A \mid\equiv \#(K_S),\quad A \mid\equiv \#(T_B)$

$B \mid\equiv \#(R_B),\quad B \mid\equiv \#(T_A),$

$A \mid\equiv \Phi(A),\quad B \mid\equiv \Phi(B)$

$A \ni K_S,\quad A \ni -SA,\quad B \ni -SB$

$A \mid\equiv A \xleftrightarrow{K_S} B,\ B \mid\equiv A \Rightarrow A \xleftrightarrow{K_S} B$

$B \mid\equiv A \Rightarrow A \mid\equiv *,\ A \mid\equiv B \Rightarrow B \mid\equiv *$

(2) 이상화된 프로토콜 및 메시지 분석

메시지는 A, B 사이에 3 단계로 구성되며, 키를 생성한후 B에게 통보하며, B는 이를 수신하여 A에게 응답을 보내주고, A는 다시 이에대한 응답을 보내주는 형식을 취한다. 이 프로토콜을 GNY 로직에서 요구하는 형태로 이상화 시켜서 각 메시지 별로 분석해 보면 다음과 같다.

1. $B \lhd : *B, *T_A, *\{B, R_A, K_S\}_{-SA}$
   $\hookrightarrow A \mid\equiv A \xleftrightarrow{K_S} B$

2. $A \lhd : *A, *T_B, *\{A, R_B, K_S\}_{-SB}$
   $\hookrightarrow B \mid\equiv A \xleftrightarrow{K_S} B$

3. $B \lhd : B, R_B$

① 메시지 1

- 규칙 T1, P1, P3, 가정 $B \ni -SB$, P8에 의해서 다음을 얻는다.

$$B \ni K_S \tag{4.1}$$

- 규칙 P1, P2 와 (식 4.1)에 의해 다음을 얻는다.

$$B \ni (B, T_A, R_A, K_S) \tag{4.2}$$

- 규칙 R1, 가정 $B \mid\equiv \#(T_B)$에 의해 다음의 결과를 얻는다.

$$B \mid\equiv \Phi(B, T_A, R_A, K_S) \tag{4.3}$$

- 규칙 F1, 가정 $B \mid\equiv \#(T_B)$에 의해 다음을 얻는다.

$$B \mid\equiv \#(B, T_A, R_A, K_S) \tag{4.4}$$

- 가정 $B \mid\ni PA,\ B \mid\equiv \xrightarrow{+PA} A$와 (식 4.3)을 규칙 I4에 적용하면 다음의 결과를 얻는다.

$$B \mid\equiv A \mid\sim (\langle K_S \rangle, R_A),$$
$$B \mid\equiv A \mid\sim (\langle K_S \rangle, R_A)_{-SA} \tag{4.5}$$

- 가정 $B \mid\equiv A \Rightarrow A \mid\equiv *$와 (식 4.4), (식 4.5)를 규칙 J2에 적용하면 다음의 결과를 얻는다.
  이것은 A가 세션키 K_S를 신뢰하고 있다는 사실을 B가 확증하였음을 의미한다.

$$B \mid\equiv A \mid\equiv A \xleftrightarrow{K_S} B \tag{4.6}$$

- 가정 $B \mid\equiv A \Rightarrow A \xleftrightarrow{K_S} B$와 (식 4.6)을 규칙 JI에 적용시키면 다음의 결과를 얻는다. 이는 B가 세션키 K_S를 신뢰하게 되었음을 의미한다.

$$B \mid\equiv A \xleftrightarrow{K_S} B \tag{4.7}$$

② 메시지 2

- 규칙 T1, P1, P3, P8 가정 $A \ni -K_{SA}$에 의해서 다음의 결과를 얻는다.

$$A \ni T_B,\ A \ni K_S,\ A \ni R_B \tag{4.8}$$

- 규칙 T1, P1, P2 와 (식 4.8)에 의해 다음의 결과를 얻는다.

$$A \ni (T_B, K_S, R_B) \tag{4.9}$$

- 규칙 R1, 가정 $A \mid\equiv \Phi(A)$에 의해 다음의 결과를 얻는다.

$$A \mid\equiv \Phi(A, T_B, B_B, K_S) \tag{4.10}$$

- 규칙 F1, 가정 $A \mid\equiv \#(T_B)$에 의해 다음의 결과를 얻는다.

$$A \mid\equiv \#(A, T_B, B_B, K_S) \tag{4.11}$$

- 가정 $A \ni PB$, $A \mid\equiv \xrightarrow{+PB} B$와 (식 4.10)을 규칙 I4에 적용하면 다음 결과를 얻는다.

$$A \mid\equiv B \mid\sim (\langle K_S \rangle, R_B)$$
$$A \mid\equiv B \mid\sim (\langle K_S \rangle, R_B)_{-SB} \tag{4.12}$$

- 가정 $A \mid\equiv B \Rightarrow B \mid\equiv *$와 (식 4.11), (식 4.12)를 규칙 J2에 적용시키면 다음의 결과를 얻는다. 이것은 B가 세션키 K_S를 신뢰하고 있다는 사실을 A가 확증하였음을 의미한다.

$$A \mid\equiv B \mid\equiv A \xleftrightarrow{K_S} B \tag{4.13}$$

③ 메시지 3

- 규칙 T1, P1, P3, P8에 의해서 다음의 결과를 얻는다.

$$B \ni R_B$$

(3) 검증 결과

GNY 로직을 통하여 얻은 결과를 정리해보면 다음과 같다.

$$B \ni K_S,\ B \mid\equiv A \xleftrightarrow{K_S} B,\ B \mid\equiv A \mid\equiv A \xleftrightarrow{K_S} B$$

$$A \ni K_S,\ A \mid\equiv A \xleftrightarrow{K_S} B,\ A \mid\equiv B \mid\equiv A \xleftrightarrow{K_S} B$$

A가 세션키 K_S를 생성하므로 A가 세션키 K_S를 소유하는 가정이 성립되며, A가 세션키 K_S를 신뢰하게 되는 것은 자연스러운 일이다. 인증절차를 통하여 또한 세션키 K_S를 소유하고 신뢰하게 되는 것을 검증 결과로 알 수 있다. 또한 A와 B 모두 상대방이 세션키를 신뢰한다는 사실을 확증하고 있음을 검증결과는 보여준다. 이것은 A와 B가 상대방을 인증하고 세션키 분배가 안전하게 이루어졌음을 보여준다. 여기서 위의 결론은 메시지 1과 2에 의해서 추론되어진 것으로 ATM의 점대 다중 방식에 메시지 1, 2를 적용하여 인증과 키분배를 수행하여도 안전성에 문제가 없는 것으로 분석되었다.

4. 결 론

본 논문에서는 ATM 망에서의 정보보호 구조를 제시하였다. ATM은 물리계층, ATM 계층, AAL 계층으로 구성된다. 그러나 정보보호를 위한 기능을 추가하면서 기존의 시스템에 영향을 주어서는 않된다. 이를 위하여 AAL 계층의 CS와 SAR 부계층 사이에 ASP 부계층의 추가를 제안하였다. ASP 부계층은 CS와 SAR에 투명하게 동작하여 기존의 고유 기능들을 만족시키면서 정보보호 기능을 수행할 수 있는 장점을 갖는다.

ATM에서의 호설정시 접속되는 VC는 인증 되지 않은 상태로 사용되기 때문에, 사용자를 검증하지 않고 통신을 시작하는 위험이 따른다. ATM 호 접속 방식에는 점대점과 점대 다중 방식이 존재한다. 점대점 방식은 "Set-Up", "Connect", "Connect Ack."의 세 가지 메시지로 구성되며, 점대 다중은 "Add Party", "Add Party Ack."의 두 가지 메시지로 구성된다. 이는 점대점 방식은 세 단계의 메시지 내에서, 점대 다중 방식은 두 단계의 메시지 내에서 인증 및 키 교환 절차를 수행해야 함을 의미한다.

본 논문에서는 또한 점대점 및 점대 다중의 호 접속시 적용할 수 있는 인증 및 키분배 프로토콜을 제안하였다. 이 프로토콜은 3단계로 구성된다. 점대점에서는 단계 3까지 적용하여 보다 강한 인증을 수행하며, 점대 다중에서는 2단계까지만 적용하여 상대방을 인증한다. 적용한 프로토콜을 L. Gong등이 제안한 GNY 로직으로 검증한 결과 프로토콜의 단계 2 까지만 적용하여도 상대방을 인증할 수 있음을 확인하였다.

참 고 문 헌

[1] Daniel Stevenson, Nathan Hillery, and Greg Byrd, Secure communication in ATM Networks,

Communications of the ACM, Vol.38, No.2, pp. 46-52, February 1995.

[2] Robert H. Deng, Li Gong, Aurel A. Lazar, Securing Data Transfer In Asynchronous Transfer Mode Networks, IEEE GLOBECOM '95, 1995.

[3] Shaw-Cheng Chuang, Securing ATM Networks, 3rd ACM Conference on Computer and Communication Security, pp.19-30, March, 1996.

[4] Li Gong, Roger Needham, Raphael Yahalom, "Reasoning about Belief in Cryptographic Protocols", Proceedings of IEEE Symposium on Research in Security and Privacy, pp.234-248, 1990

[5] Michael Burrows, Martin Abadi, Rodger Needham, "A Logic of Authentication", ACM Transactions on Computer Systems, pp.18-36, Vol.8, No.1, Feb. 1990.

[6] Hyo-Young Shin, Hwang-Bin Ryou, "A study for providing confidentiality in ATM", Proceedings of JW-ISC '97, Oct. 1997.

[7] 신효영, 유황빈, "ATM 방식의 고속 통신망에서 비밀성 보장을 위한 구조와 암호 알고리즘에 관한 연구", 한국통신학회 논문지, 23권 1호, pp.168-178

신 효 영

e-mail : hyshin@cs.kwangwoon.ac.kr

1986년 2월 광운대학교 전자계산학과(이학사)

1988년 2월 광운대학교 대학원 전자계산학과(이학석사)

1998년 8월 광운대학교 대학원 전자계산학과(이학박사)

1988년~1993년 LG 소프트웨어(주)

1994년~현재 경복대학 사무자동화과 조교수

관심분야 : 컴퓨터 네트워크, 네트워크 보안, 멀티미디어 통신

유 황 빈

e-mail : ryou@cs.kwangwoon.ac.kr

1975년 2월 인하대학교 전자공학과(공학사)

1977년 7월 연세대학교 대학원(공학석사)

1989년 2월 경희대학교 대학원(공학박사)

1994년 2월~1995년 2월 美 UCSD 교환교수

1995년~1997년 광운대학교 전자계산소장

1981년~현재 광운대학교 컴퓨터과학과 교수

1995년~현재 광운대학교 신기술연구소 연구원

1997년~현재 광운대학교 중앙도서관장

관심분야 : 네트워크 보안, 멀티미디어 통신, VOD