# ATM 기반 IP 네트워크에서의 위협요소 분석 및 보호방법

김도완*, 김기현**, 한치문*
*한국외국어대학교 전자공학과, **한국정보보호센터
전화 : (0335) 330-4503

# Security Solution and Threats Analysis in the ATM based IP Network

Do Wan Kim*, Kee Hyun KIM**, and Chimoon HAN***
*HUFS,kd0901@san.hufs.ac.kr, **KISA,danny@kisa.or.kr, and ***HUFS cmhan@maincc.hufs.ac.kr

## Abstract

This paper describes on the threats such as IP spoofing, denial of service, and ILMI based attack etc. for IP over ATM network. Especially we discuss on the threats due to ATM characteristics that are VC stealing, multiparty and multi-connection call. Also we investigate on the threats of ATM based MPLS network. Finally we discuss and suggest the various solutions of ATM security.

## 1. 서 론

현재의 인터넷망은 사용자의 급증으로 인한 트래픽의 정체, 속도의 저하 등으로 미래의 멀티미디어 서비스 제공에 적합하지 못하다. 따라서 앞으로의 멀티미디어 서비스와 고속의 통신을 위해서 ATM망을 기반으로 한 IP통신이 주류를 이룰 것이다. 그러나 최근에 새로운 해킹 방법들이 다양화, 지능화되어 이전의 시스템에 대한 보안 방법으로는 ATM 망과 기존의 패킷망과의 연동으로 발생하는 취약점에 대한 방어가 어렵다. 또한 인터넷 서비스의 활성화로 전자상거래, 전자 경매 등과 같은 중요한 정보의 유통이 IP over ATM 방식으로 이루어 질 것이다. 따라서 본 논문에서는 ATM망 자체의 보안 취약점과 이를 기반으로 한 IP망에서의 공격가능성에 대한 위협요소를 분석하고, 이에 대한 보호 방법을 조사한다.

2장에서는 IP over ATM 방식에서 ARP 서버의 주소 등록 과정에서의 위협요소와 ATM 스위치와 단말기 간의 인터페이스인 ILMI에 의한 주소 자동설정시의 위협요소, 공격자가 네트워크 자원의 선점으로 인한 사용자의 서비스를 제공하지 못할 가능성 그리고 ATM 망이 가지는 특성을 이용한 공격 가능성에 대해 분석한다. 또 ATM 기반 MPLS 네트워크에서의 위협요소를 간단히 정리한다. 3장에서는 위협 요소들에 대한 보호 방법으로 ARP 서버에 인증절차나 방안과 SNMP가 자동 주소 설정시에 사용하는 신호 메시지를 암호 알고리즘을 이용하여 암호화하여 통신하는 방안, 망자원에 대한 접근제어 방식으로 서비스 이용자의 서비스 액세스를 제한하는 방법들에 대해 설명한다. 그리고 ATM 보안 프레임에서 제안한 인증, 무결성, 기밀성, 가용성, 책임성 개념을 포함한 ATM 네트워크 설계가 ATM 네트워크에서의 위협 요소에 대한 한 방안임을 확실히 한다.

본 논문은 1999년도 한국정보보호센터가 지원하는 "정보통신 기반구조보호기술 개발" 사업 수행 결과의 일부입니다.

## 2. ATM 기반 IP에 대한 위협요소

### 2.1 ARP서버의 취약점을 이용한 공격

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

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, ① ARP는 In *ATM ARP request* 메시지를 단말로 보낸다. ②이 메시지를 수신한 단말은 자신의 IP 주소와 ATM 주소가 포함된 *In ATM ARP* 메시지로 응답한다. ③ ARP는 이 정보를 가지고 ARP 테이블을 변경한다. 이 때 공격자는 공격하고자 하는 IP 주소를 자신의 IP 주소로 등록하게 되면, 공격 당한 IP 주소로 보낸 모든 정보는 공격자 단말로 전달될 것이다. 이 과정을 그림1에 나타냈다.

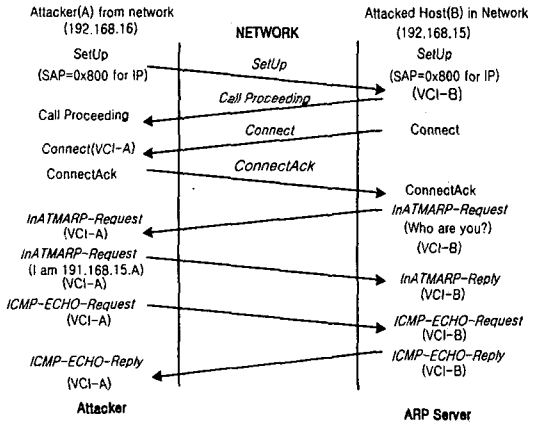


그림1. IP Spoofing 과정

## 2.1 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 IP정보를 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 MIB정보를 지운다.

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

③ ILMI는 자동적인 Configuration절차를 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.

## 2.2 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.

## 2.3 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. 그림2와 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. 이러

한 공격은 양단의 스위치에서 라우팅 테이블 변경으로 가능하다. 이러한 발생은 동일 사업자가 제공하는 망에서는 가능성이 낮지만, 서로 다른 망 사업자간의 연동시에 일어날 가능성이 높다.

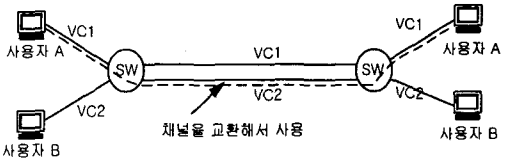


그림2. ATM 네트워크에서의 VC 도용

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, 공격자는 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.

## 2.4 ATM 기반 MPLS에서 위협

ATM 기반 MPLS 네트워크 구성은 그림3과 같다. 그림3에서 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.

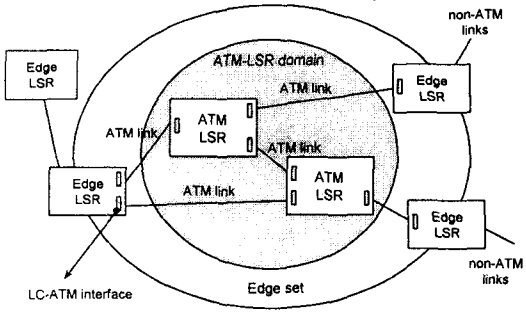


그림3. ATM based on MPLS Network 모델

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.

## 3. 해결 방법( Security Solution) 검토

### 3.1 ARP서버에 인증 절차 도입

2장에서 기술한 ARP서버에서 각 단말의 IP 주소와 ATM 주소의 등록과정에서 존재하는 위협은 주소등록시에 인증절차를 거치게 함으로써 방어가 가능하다. 또 ARP 서버의 테이블 내용을 정적 구조를 갖도록 구성한다. 그리고 ARP 서버에 커넥션 설정한 후, ARP서버는 자신이 속해있는 LIS내의 각 단말에게 *In-ATM ARP request* 메시지를 보내면, 단말들은 자신의 IP주소와 ATM 주소를 *In-ATMARP* 메시지로 응답하여 등록하게 된다. 이때 ARP 서버 내에 인증 기능을 설치해서 현재 등록된 주소 테이블에서 IP 주소와 ATM 주소를 비교한 후, 중복된 주소를 찾아내서 나중에 등록하려는 단말의 등록을 거부하는 방식으로 공격자의 위조된 IP 주소 등록을 방지한다[그림4].

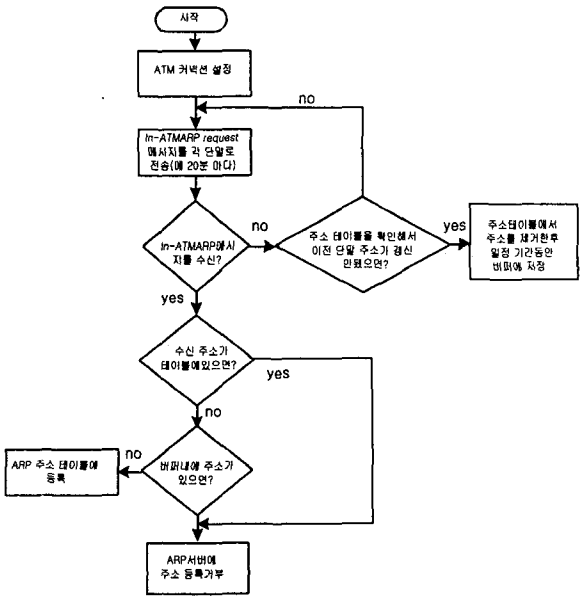


그림4. 정적 구조를 갖는 ARP 서버의 인증 절차

그리고 ARP 서버에 새로운 엔트리(ATM주소-IP주소) 등록은 공격자 혹은 새로 설치하는 가입자일 것이

다. 따라서 새로 등록을 요구할 경우에는 ARP 서버에서 상호 인증기능을 갖도록 한다. 정기적인 주소 갱신 시 테이블에 삭제된 주소를 일정기간 동안 버퍼에 저장시킨 후, 새로운 주소로 등록을 하려는 단말의 주소와 비교함으로써, 공격자가 의도적으로 자신의 ATM 주소를 가지고 공격을 원하는 단말의 IP 주소로 등록하여 IP 도용하는 것을 방지할 수 있다.

### 3.2 SNMP 메시지의 암호화

ILMI에서 SNMP 메시지를 사용하여 UNI 신호를 NNI 신호로 변환하여 오프라인 된 단말기의 주소를 등록시키는 공격 방법은 스위치와 ILMI간의 모든 SNMP 메시지를 암호화 알고리즘을 사용해서, 암호화하여 통신하게 되면, 이 메시지를 조작하여 P-NNI 라우팅 프로토콜을 사용하는 것처럼 가장하는 것을 막을 수 있다.공개키 암호를 기반으로 한 알고리즘(예: X.509, DES-CBC)을 사용하여 메시지를 송수신하게 되면, 외부의 공격자가 암호화된 SNMP 메시지를 가로채서 replay 공격을 하더라도 방어가 가능하다[그림5]. 그리고 단말기와 ATM 스위치와의 자동주소 설정 시의 신호 메시지도 암호화 알고리즘을 적용하여 안전성을 증가 시킬 수 있다. 하지만 이 방법은 라우팅 속도의 저하와 암호키에 대한 버퍼의 필요로 인해 메모리가 증가하는 단점이 있다.

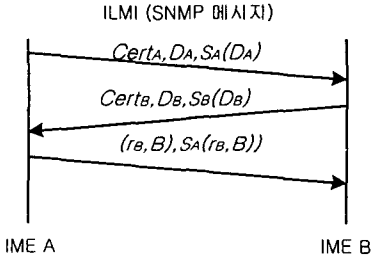


그림5. X.509 three way 방식으로 암호화 예

### 3.3 접근제어 신호를 이용한 접근 제한

네트워크 자원선점에 의한 서비스 거부의 대책으로는 ATM 스위치에서 접근제어(access control)신호를 이용하여 사용자의 권한을 제한함으로써 방어를 할 수 있다. 공격자의 IP 할당에 의한 서비스 거부에 대한 보호는 LIS내의 시스템 관리자가 미 사용중인 IP주소를 미리 할당하였다가 사용자가 필요할 때, 재 할당하는 방법이 있다. 그리고 ARP 서버에서 *In-ATM ARP* 메시지로 단말에서 IP, ATM 주소를 의뢰할 때, 이 횟수를 제한하여 공격자가 미 사용자중인 IP주소를 알아내지 못하게 하는 방법 등을 생각할 수 있다.

대역폭의 선점 할당에 대해서도 시스템 관리자가 한 사용자의 CBR 대역폭 할당을 제한하여, 모든 대역폭을 공격자에 의해 할당하는 것을 방지할 수 있다. 그러나 망 관리자에 권한이 집중되어 있으므로 관리자의 비밀번호가 노출되어 공격자가 권한을 획득할 경우, 피해가 커질 가능성이 있다. 또 다른 방법은 모든 VC를 PVC로 할당함으로써 방지할 수 있다. PVC의 할당은 자원의 효율적인 이용이 이루어지지 않는 단점이 있다.

VPI나 VCI 선점 할당에 대한 해결 방법은 접근제어. 신호를 이용하여 스위치 입력단에서 VPI/VCI가 특정 포트에 모두 할당되는 것을 방지하는 것이다. 즉 ATM 스위치의 특정 포트가 가질 수 있는 VPI/VCI의 역치를 설정하고, 이 값을 초월하지 않도록 제어함으로써 어느 정도 해결 할 수 있다.

### 3.4 SA(Security Agent)를 사용한 ATM 네트워크 보안 메커니즘 설계 및 적용

ATM망의 특성에 따른 공격은 ATM 보안 프레임워크에서 제안한 인증(Authentication), 데이터 무결성(Integrity), 기밀성(Confidentiality), 책임성(Accountability), 가용성(Availability)을 연합 또는 각각을 단독으로 설계하여 구현함으로써 ATM 망에 대한 보안을 보장할 수 있다. 특히 적용하고자 하는 보안범위에 SA(Security Agent)를 설치하여 SA간에 필요한 보안 파라미터 협상을 통해 이루어진 보안 메커니즘에 근거하여 통신을 하면,

지금까지 언급한 ATM 위협 요소에 대한 방어가 가능하다. SA는 양 단말사이에 또는 스위치간에 설치가 가능하며, 보안의 견고성을 강조하기 위해 SA를 여러 개 네스팅하는 방식도 적용될 수 있다. 또 사용자 데이터 보안과 더불어 제어 신호, 망관리 정보의 보안이 필요하다.

## 4. 결 론

본 고에서는 ATM 망을 기반으로 하는 IP 통신 방식에 대한 위협 요소 및 ATM 망 특성에 기인한 위협 요소들에 대해 언급하였다. ATM 망과 기존의 망과의 결합에서 생기는 보안상 취약점은 주소 변환 등의 과정이 자동적으로 인증 없이 수행되기 때문에 발생하게 된다. 이에 대한 해결방법으로 메시지의 암호화, 인증 절차의 설치 및 강화, 접근제한 등을 통해 가능하다. 이러한 기술들은 현실적으로 사용하기에 오버헤드나 복잡한 절차 등으로 속도가 떨어지거나 가격이 올라 갈수도 있다. 또한, 이러한 것들은 네트워크 설계 후에 보안 서비스에 대해 고려하는 방식이기 때문에 망에 대한 보안상 취약점이 생기고, 효율적인 보안이 이루어지지 않는다. 따라서 ATM 네트워크에서 요구되는 보안 메커니즘 개발이 필요하며, 이에 대한 지속적인 연구가 요구된다.

### [ 참고문헌 ]

[1] ATM Forum Technical Committee, "ATM Security Framework 1.0" February 1998.

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

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

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