ATM-Metro 서비스 보안성 분석

노선식*, 조정호*, 이동은**

*광주대학교 정보통신학과, **청운대학교 인터넷컴퓨터학과

A Study on The Security of ATM-Metro Service

Sun-Sik Roh*, Jung-Ho Cho*, Dong-Eun Lee**

* Dept. of Information & Communication Engineering. Gwangju Univ.

** Dept. of Internet Computer. Chungwoon Univ.

E-mail : ssroh@gwangju.ac.kr

요 약

본 논문에서는 광대역통합국가망에서 ATM-Metro 서비스의 망 구조 및 서비스 제공 방식을 분석한다. ATM-Metro 서비스를 제공함에 있어서 존재하는 보안 취약점 및 보안 공격을 분석하며, 이를 기반으로 안전하게 ATM-Metro 서비스를 제공하기 위한 일반적인 보안 강화 방안을 제시하고, ATM 접속 방식과 이더넷 접속 방식의 ATM 구간에서 보안 기능을 강호하기 위한 보안 모델을 제시한다. 또한 ATM-Metro Ethernet 구간에서 기본적인 보안 기능을 제공할 수 있는 VLAN 적용 방안을 제시하고, ATM-Metro 서비스 전구간에서 보안성을 강화할 수 있는 방안을 제시한다.

Ⅰ. 서 론

광대역통합국가망은 ATM PVC/SVC 서비스, 전용회선 서비스, 프레임릴레이서비스, 패킷교환 서비스 등 다양한 전송 서비스를 제공하고 있으며, 이를 통해 이용기관들이 통신 서비스나 인터넷 서비스를 이용할 수 있다[1-2]. 하지만 대부분의 이용기관이 이더넷 망을 구축함으로써, 이더넷 인터페이스가 아닌 다른 방식으로 광대역통합국가망에 접속할 경우 추가적인 부담을 갖게 된다. 그래서 이용기관으로 하여금 이더넷 인터페이스를 통해 접속할 수 있도록 ATM-Metro 서비스를 제공한다[3].

ATM-Metro 서비스는 Ethernet-ATM 장비를 기반으로 가입자의 이더넷 트래픽을 ATM 트래픽으로 전화하여 ATM 교환망으로 전송한다. 즉 ATM-Metro 서비스는 ATM 전송 방식과 이더넷 전송 방식이 공존하게 된다. 이로 인해 두 전송 방식의 보안 취약점이 동시에 존재하게 되므로, 다양한 보안 공격이 가능하다. 따라서 ATM-Metro 서비스의 확산을 위해서는 이용 기관의 보안에 대한 불안을 해소할 수 있는 보안 기능의 강화가 필수적으로 요구된다.

본 논문에서는 ATM-Metro 서비스 구간에서 안전한 서비스 제공을 위한 보안 강화 방안을 제시한다. ATM-Metro 서비스 망의 구조 및 서비스 제공 방식을 분석함으로써, ATM-Metro 서비스에 존재하는 보안 취약점 및 보안 공격을 분석하고, 안전하게 ATM-Metro 서비스를 제공하기 위한 보안 요구 사항을 도출한다. 이더넷 구간에서 기본적인 보안 기능을 제공하기 위한 구조적인 방안을 제시하고, ATM-Metro 전구간에서 보안을 강화할 수 있는 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 ATM-Metro 서비스에 대하여 기술하고, 3장에서 ATM-Metro 서비스 제공할 때 존재하는 보안 취약점에 대하여 기술한다. 4장에서는 ATM-Metro 서비스의 보안 요구 사항 및 보안성 강화를 위한 방안을 제시한다.

Ⅱ. ATM-Metro 서비스

광대역통합국가망에서 핵심 전송망인 ATM 교환망의 서비스 이용 활성화를 위하여 ATM-Metro 서비스를 제공하고 있다[3]. ATM-Metro 서비스는 광대역통합국가망의 이용 기관들이 이더넷 접속 방식 즉 이용 기관의 장비에 이더넷 포트만 있으면 광대역통합망을 통해 기관간 통신 및 인터넷 통신을 이용할 수 있는 서비스이다. 즉 이용 기관이 광대역통합국가망에 접속하기 위해서 새로운 장비의 도입 없이 기존 구내망의 이더넷 환경을 이용하기 위한 서비스이다.

ATM-Metro 서비스에서 이용기관과 광대역통합국가망은 물리적으로 1:1 접속관계를 갖으며,

접속은 이더넷 방식으로 하고 내부는 ATM PVC/SVC 서비스를 이용하여 전송함으로 이더넷의 경제성과 ATM의 보안성 확보가 가능하다. 그림 1은 ATM-Metro 서비스망 구성도를 나타낸다.

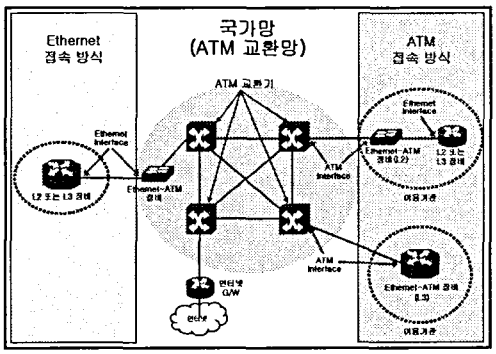

그림 1. ATM-Metro 서비스 망

Ethernet-ATM 장비는 이용기관과 ATM 교환망의 인터페이스를 담당한다. 이용기관은 이더넷을 통해 Ethernet-ATM 장비에 접속하며, 광대역통합국가망에서는 ATM 방식을 이용하여 Ethernet-ATM 장비에 접속한다. ATM-Metro 서비스는 Ethernet-ATM의 위치에 따라 ATM 접속 방식과 이더넷 접속 방식으로 구분된다.

이더넷 접속 방식은 Ethernet-ATM 장비가 광대역통합국가망 내부에 위치하는 방식으로, 이용기관이 이더넷 방식으로 접속하며 이더넷과 ATM의 전환을 광대역통합국가망 내부에서 수행하는 방식이다. 이용기관과 Ethernet-ATM 장비는 광케이블을 통해 연결되고, 기존 이용기관의 L2/L3 장비와 광테이블을 연결하기 위해서는 컨버터 장비가 필요하다.

ATM 접속 방식은 Ethernet-ATM 장비가 이용기관관 내부에 위치하는 방식으로 이더넷과 ATM의 데이터 전환을 이용기관 내부에서 수행하는 방식이다. ATM-Metro 서비스 이용기관 접속장비의 주요기능은 표1과 같다.

III. ATM-Metro 서비스 보안 취약점

ATM-Metro 서비스는 Ethernet-ATM 장비를 기준으로 이용기관이 이더넷을 이용하여 접속하는 이더넷 구간과 ATM을 이용하여 접속되는 ATM 구간으로 구분된다. ATM 구간은 광대역통합국가망의 전송망인 ATM 교환망을 포함한다.

ATM 구간은 이용기관의 이더넷 트래픽이 전환된 ATM 셀을 ATM 전송 방식으로 전송한다. 이로 인해 ATM 구간은 ATM 전송 특성에 의한 다음과 같은 보안 취약점이 존재한다.

표 1. ATM-Metro 서비스 접속장비

구분	접속장비	주요기능
ATM방식	Ethernet-ATM 장비	가입자 측의 이더넷 패킷과 망 측의 ATM 셀을 상호 변환하여 광대역통합국가망 내부의 ATM-MUX와 연결하는 기능을 수행
	Ethernet-Router	L3(라우터) 기능을 수행하고 가입자 댁내에 위치한 Ethernet-ATM 장비와 연결하는 기능을 수행
	ATM-Router	L3(라우터) 기능을 수행하고 가입자 측의 이더넷 패킷과 망 측의 ATM 셀을 상호 변환하여 광대역통합국가망 내부의 ATM-MUX와 연결하는 기능을 수행
이더넷방식	Ethernet-Router	L3(라우팅) 기능을 수행하고 국가망 내부에 위치한 Ethernet-ATM 장비와 연결하는 기능을 수행하는 장비

• 도청: Ethernet-ATM 장비를 통해 전환된 ATM 셀은 ATM 전송 방식에 따라 광케이블을 통해 가입자 ATM 교환기에 전송된다. Ethernet-ATM 장비는 단순히 이더넷 데이터를 ATM 셀로 전환하는 기능만을 수행하기 때문에, 광전송특성을 이용한 도청이 가능하다.

• 주소 매핑을 이용한 스푸핑 공격: ATM이나 이더넷을 기반으로 하고 있는 인터넷 통신에서는 IP 주소를 ATM 주소나 이더넷 주소로 매핑하는 과정이 필요하다. 또한 ATM-Metro 서비스에서는 이더넷 주소를 ATM 주소로 매핑하는 과정이 필요하다. ATM-Metro 서비스를 제공하기 위해서는 ATM 연결이 먼저 설정되어야 하므로, ATM 주소는 고정되게 되며 공격자는 이용기관의 IP 주소나 이더넷 주소로 위장하여 데이터를 전송하는 스푸핑 공격이 가능하다.

• 망자원선점에 의한 DOS(Denial of Service) 공격: ATM 구간은 ATM PVC 서비스를 통해 전송된다. 하지만 이용기관의 수가 늘어나고 트래픽양이 증가하게 되면 ATM SVC 서비스를 통해 서비스를 제공해야 한다. 이때 특정 이용기관이 VPI 또는 VCI를 선점하게 되면, 다른 이용기관은 서비스를 제공받지 못하게 된다.

• 인증되지 않은 트래픽 전송: Ethernet-ATM 장비를 통해 전환된 ATM 셀은 ATM 교환망에서 인증 절차 없이 전송된다. 이때 공격자가 임의의 이더넷 프레임을 Ethernet-ATM 장비로 전송함으로써 허가 없이 ATM 교환망을 통해 데이터를 전송할 수 있다.

ATM-Metro 서비스 이용기관들은 이더넷 기술을 기반으로 하여 광대역통합국가망에 접속한다. 이더넷 방식은 설계 단계에서 보안성을 고려하지

않았기 때문에 다양한 보안 위협이 존재한다. 첫째, 망을 구성하는 모든 노드들은 하나의 물리적 채널을 공유하고, 브로드캐스트 방식을 이용하여 데이터를 전송함으로써 이더넷 상의 모든 트래픽은 도청이 가능하다. 둘째, 노드들이 데이터를 전송할 때 전송 시간이나 공유 매체에 대한 사용시간을 제한할 수 없으므로 서비스거부공격이 가능하다. 셋째, 이더넷 방식은 메시지 송신자에 대한 인증과 메시지의 무결성 기능을 제공할 수 있는 방법을 제공하지 않는다. 이러한 보안 위협에 대응하기 위해 제안된 것이 VLAN(Virtual LAN)이다[4].

VLAN은 서로 관련된 사용자들을 물리적인 접속에 관계없이 그룹화하여 구성하는 방법이다. 하나의 VLAN에 속해 있는 노드는 다른 VLAN에 속해 있는 노드와 통신을 하지 못하며, 다른 VLAN 트래픽을 수신할 수 없기 때문에 이더넷에서 보안 기능을 제공할 있다. 따라서 ATM-Metro 서비스의 이더넷 구간에서 보안 기능을 제공하기 위해서는 VLAN 기능을 제공해야 한다. 하지만 VLAN을 ATM-Metro 서비스에 적용함에 있어서 다음과 같은 보안 위협이 존재한다.

• Lookup Table Overflow: ATM-Metro 서비스에 VLAN을 적용하게 되면, VLAN에 대한 ID와 관련된 정보들을 저장하여 관리하게 된다. 이때 관련 정보 저장 공간이 제한되어 있으므로 다량의 위조된 정보를 통해 Lookup Table Overflow가 가능하며, 이로 인해 다른 모든 노드가 패킷을 수신할 수 있게 된다.

• 태깅공격: 트렁크 포트를 이용하여 한 VLAN에 속해 있는 사용자가 다른 VLAN에 대한 접근을 허용하도록 하는 공격이다.

• 중복캡슐화공격: VLAN을 사용하여 스위치간에 통신을 하기 위해서는 802.1q를 사용한다. 이때 공격자가 공격을 위한 패킷을 802.1q 태그를 이용하여 중복 캡슐화할 경우 목적지 스위치에서는 원래의 태그 정보가 아닌 중복된 태그 정보에 의해 패킷을 전송하게 된다(그림2).

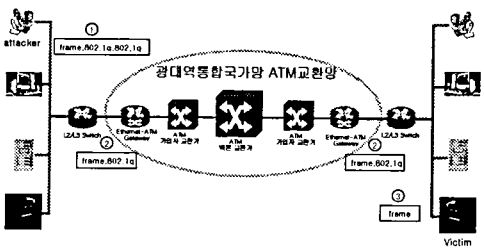

그림 2. 중복 캡슐화 공격

IV. Metro-ATM 서비스 보안 강화

가. 일반적인 보안 강화

ATM-Metro 서비스를 제공함에 있어서 일반적으로 다음과 같은 보안 기능이 제공되어야 한다.

• ATM-Metro 서비스 구간에서 접속 라인의 장애는 ATM-Metro 서비스 및 광대역통합국가망의 서비스를 제공하지 못하게 한다. 라인의 장애가 있을 경우 백업 라인을 이용하고, 주 통신 라인과 백업 라인의 전환이 쉽게 이루어질 수 있도록 라인 관리 기능을 제공함으로써 ATM-Metro 서비스의 가용성을 제공해야 한다.

• 보안 공격을 하기 위해서는 ATM-Metro 서비스 통신망에 접속해야 하다. 따라서 Ethernet-ATM 장비 등 ATM-Metro 서비스 이용기관 접속 장비에 대해 특정 사용자의 물리적인 접근을 엄격하게 통제해야 한다(물리적인 접근제한).

• Ethernet-ATM 장비 등 ATM-Metro 서비스 이용기관 접속 장비들은 시스템 패스워드 설정, 엄격한 로그인 기능 제공, 멀티레벨 사용자에 대한 계정 관리, 콘솔/망 접근에 대한 자동 제어 기능 등을 제공하는 일반적으로 증명된 보안 도구를 사용하여 자체적인 보안 기능을 강화해야 한다.

나. ATM 구간 보안 강화

ATM 망에서 인증, 기밀성, 무결성, 접근 제어 등 보안 서비스를 제공하는 ATM 망 구성 요소가 ATM 보안 장비이다[5-7]. 일반적으로 ATM 보안 장비는 사용자와 공중 ATM 망 사이에 위치하여 다양한 보안 서비스를 제공한다. 사용자의 가상 채널 연결 요청을 수신하여 보안 연결을 설정하며, ATM 셀에 대해 암호화/복호화를 수행하여 데이터 기밀성을 제공한다. 또한 암/복호화를 위해 필요한 세션키를 생성/분배하며, 목적지 ATM 보안 장비와 상호 인증 및 전송되는 정보의 무결성을 보장하기 위한 보안 서비스를 수행한다.

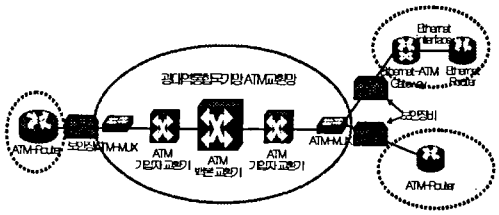

그림 3. ATM 접속 방식의 보안 모델

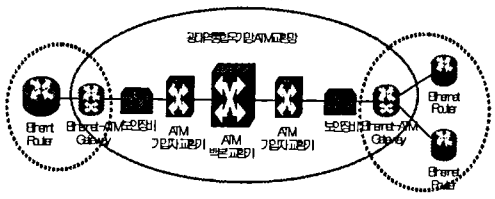

그림 4. Ethernet 접속 방식의 보안 모델

기존의 ATM 보안 모델을 광대역통합국가망의 ATM-Metro 구간에 적용할 경우 ATM-Metro 서비스에 대해서 ATM 보안 장비는 그 기능을 제공하지 못한다. 따라서 ATM-Metro 서비스를 제공하기 위한 Ethernet 접속 방식과 ATM 접속 방식에 있어서 ATM 보안 장비는 Ethernet-ATM 장비의 광대역통합국가망 접속 부분에 설치되어 Ethernet-ATM 장비에 의해 생성된 ATM 셀에 대하여 보안 기능을 수행해야 한다. 그림 3.은 ATM 접속 방식의 보안 모델을 나타내며, 그림 4.는 이더넷 접속 방식의 보안 모델을 나타낸다.

다. 이더넷 구간 보안 강화

이더넷 구간에서 기본적인 보안 기능은 VLAN을 사용함으로써 제공할 수 있다. VLAN은 한 사이트 또는 이용기관 안에서 VLAN을 적용하는 것보다 종단간에 VLAN을 적용하면 더욱 강화된 보안 서비스를 제공할 수 있다. 따라서 ATM-Metro 서비스에서도 안전한 데이터 전송을 위해서는 이더넷 구간에서 VLAN을 적용해야 하며, VLAN의 적용은 종단간에 이루어져야 한다. 그림 5는 ATM-Metro 서비스의 VLAN 적용 모델을 나타낸다.

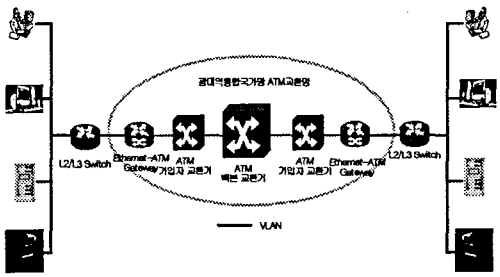

그림 5. ATM-Metro 서비스의 VLAN 적용 모델

VLAN 적용 모델을 기반으로 ATM-Metro 서비스의 이더넷 구간 보안 강화 방안은 다음과 같다.

• 기본적인 보안 서비스를 제공하기 위해서 VLAN을 사용하며, 종단간 VLAN을 사용함으로써 보안성을 강화한다.

• 프로토콜이나 트래픽에 대한 접근 제어를 이용하여 ATM-Metro 서비스 망에 대한 접근 권한을 제어하며, 특히 전송속도와 같은 속도로 접근 제어 기능을 제공해야 한다.

• 802.1x나 동적 VLAN 등과 같은 인증 메카니즘을 이용해야 한다.

• 이용기관 접속 장비의 보안 설정을 강화한다. 불필요한 포트는 임의로 이용기관에서 사용하지 않도록 제어하고, 트렁크 포트의 설정은 정해져 있는 ID를 이용한다. 불필요한 포트에 대해서는 이용기관의 사용을 철저하게 차단한다.

• 이용기관 접속 장비에 대한 안전한 관리 방법을 이용한다. 공격자가 관리권한을 갖지 않도록 하며, 접근제어나 필터를 통해 이용기관 접속 장비에 대한 접근을 통제한다. 제어프로토콜에 대해서는 QoS 등을 이용하여 우선 순위를 부여하여 관리한다.

V. 결론

이더넷을 구내 기본 망으로 사용하는 이용기관에 대하여 광대역통합국가망에 대한 편리한 접속을 제공하기 위해 ATM-Metro 서비스를 제공하고 있다. ATM-Metro 서비스는 접속 방식에 따라 ATM 접속 방식과 이더넷 접속 방식으로 구분되지만 전송 특성에 따라 ATM 구간과 Ethernet 구간으로 구분할 수 있다. ATM 구간에서는 ATM 보안 장비를 Ethernet-ATM 장비와 광대역통합국가망 접면에 배치함으로써, ATM-Metro 서비스에서 ATM 셀 전송에 따른 강화된 보안 서비스를 제공할 수 있다. 이더넷 구간에 대해서는 기본적으로 VLAN을 사용해야 하면, VLAN을 종단간에 사용함으로써 종단간 보안 기능을 강화해야 한다. 또한 VLAN에 존재하는 보안취약점에 대응하기 위해 인증 메카니즘, 접근제어, 접속 장비의 보안 설정 강화 및 보안 관리 방안을 강화해야 한다.

Acknowledgement

본 연구는 한국전산원의 지원으로 수행되었습니다.

참고문헌

[1] 정보통신부, "한국의 초고속정보통신망 발전사", 2003.5

[2] 정보통신부,"초고속정보통신망 고도화 추진계획", 2001.6

[3] 한국전산원, "ATM-Metro 서비스 접속 기준(안)", 2003.8

[4] Mathias Hein, David Griffiths, Orna Berry, "Switching Technology in the Local Network: From LAN to Switched LAN to Virtual LAN," February 1997

[5] ATM Forum Technical Committee, "ATM Security Framework 1.0", af-sec-0096.000, February, 1998

[6] ATM Forum Technical Committee, "ATM Security Specification," Version 1.0, af-sec-0100.001, February, 1999

[7] ATM Forum Technical Committee, "ATM Security Specification," Version 1.1, af-sec-0100.002, March, 2001