주 제

MPLS망에서의 정보보호

대구가톨릭대학교 **전용희**

차례

I. 서 론

광대역통합망 구축 기본계획에 의하여 초고속국가망을 고품질의 전자정부 서비스를 제공할 수 있는 품질보장망으로 고도화하기 위한 전략을 수립하여 추진하고 있다[1]. 광대역 통합망(BcN: Broadband convergence Networks)은 유 · 무선, 통신 · 방송 · 인터넷 등이 융합 수용된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊어짐 없이 안전하게 제공할 수 있는 차세대 정보통신 인프라를 말한다. 이를 위하여 BcN 전달망은 서비스 품질(QoS: Quality of Service) 보장, 고도의 통신망 관리 기능과 보안(Security) 기능, IPv6 주소체계의 수용을 통하여 다양한 서비스를 쉽게 창출할 수 있는 개방형 망구조(Open API)를 도입한 통신망으로 유선 · 무선 · 방송 등의 다양한 가입자망의 특성을 통합하여 수용해야 하며, 표준 인터페이스를 통해 다양한 응용서비스의 개발 및 이용 환경을 제공할 수 있어야 한다[2]. BcN 구축 기본계획에서, 보안 즉, 정보보호란 정보통신망 기능의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 제반 위협과 부작용 등의 정보화 역기능에 대한 대응을 의미한다[1].

새로운 애플리케이션들을 위한 서비스 요구사항을 지원하기 위하여 다른 수준의 네트워크 서비스 보장을 제공하기 위한 프레임워크 및 프로토콜들이 제안되었다. 이들 중에는 ReSerVation setup Protocol(RSVP), Differentiated Services (DiffServ), 그리고 Multiple Protocol Label Switching(MPLS) 등이 있다. 이와 같은 QoS-aware 통신 시스템에서 사용자는 각각 다른 신뢰성, 예측성과 효율성 정도를 가지고 있는 여러 가지 서비

스 클래스 중에서 선택할 수 있다. 그러나 아직 국내에서는 보안이 QoS 구조에서 하나의 파라미터로 포함되지 않고 있으며 보안-관련 서비스 클래스가 정의되지 않았다. 따라서 종단 사용자가 적절한 보안 레벨을 구성할 수 없게 된다.

보안은 1960년대 이후로 지속적으로 연구되고 있는 분야이다. QoS 영역도 많은 연구가 이루어지고 있다. 그러나 QoS의 보안 관점에 대하여는 많은 연구가 진행되지 않은 상태이며, 더구나 국내에서 BcN 보안이나 secure QoS에 관한 참고문헌을 거의 찾을 수 없는 실정이다[3]. 따라서 본 논문에서는 BcN에서 QoS를 지원할 수 있는 MPLS 통신망 구조에서 적용될 수 있는 보안 메커니즘들을 살펴보고 MPLS의 보안 특징에 대하여 분석 기술하고자 한다.

II. 광대역통합망 보안

개방형 망구조(Open API)를 지원하는 BcN은 다양한 경로를 통하여 통신망에 대한 접근이 쉽고, 이를 이용한 해킹 공격 및 바이러스 유포 등의 위험성이 존재한다. BcN에서 고려되어야 할 위협요소는 다음과 같다[3].

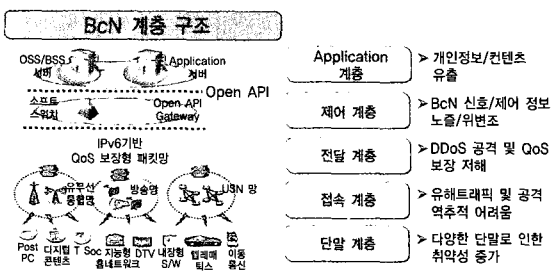
전체 통신망으로 개별 통신망에 대한 위협이 확산될 가능성이 더욱 높아진다. 기존의 개별적인 통신망에 대한 피해가 개별 통신망들이 상호 통합된 BcN 상에서는 연결된 음성통신망, 방송망, USN(Ubiquitous Sensor Network)까지 모든 구성 네트워크로 그 피해가 확산될 수 있다. 따라서 BcN 환경에서는 네트워크 전체에 대하여 체계적으로 통합 관리함으로써 신속한 대응 체계를 갖출 필요가 있다.

빠른 전송 속도로 인하여 웜과 같은 악성 코드의 확산이 가속화되어, 네트워크 공격에 대하여 대응할 수 있는 시간도 단축된다. 이에 따라 Zero-day 공격에 대응할 수 있는 No Signature IPS(Intrusion Prevention System) 등에 대한 기술 개발이 요구된다.

IPv6 기반의 BcN에서 IPv6 기능의 취약점을 이용한 새로운 공격이 발생될 가능성이 있다. 따라서 IPv4망에서 발생되었던 여러 가지 기존의 위협 형태를 포함하여 새롭게 IPv6에서 발생될 수 있는 취약점, 기존 IPv4에서 IPv6로 전환하는 단계에서 발생할 수 있는 위협이 있다.

BcN과 연결되는 USN에서의 취약점이 있다. 사용되는 CPU 용량이 적고 저전력을 사용하기 때문에 자원에 대한 DoS 공격에 취약하고, 분산되어 설치된 센서를 통한 개인정보보호 침해에 대한 문제가 발생할 수 있다.

네트워크 혹은 서비스 제공자는 위협 분석과 위험 평가의 결과를 근거로, 어떤 보안 대책을 수립할 것인지를 결정해야 한다. 그림 1은 BcN 계층별 정보보호 위협을 보여준다[4].



(그림 1) BcN 계층별 정보보호 위협

(그림 1)의 BcN 정보보호 위협에 대하여 좀 더 자세히 기술하면 다음과 같다.

- 개방형 인터페이스를 사용하는 어플리케이션 계층의 사용자 개인정보 및 개방형 서비스 구조에서 제공되는 컨텐츠에 대한 지적 재산권 침해 위협

- 과금, 인증, 정책, 설정정보와 등과 같은 중요 제어/설정 정보의 노출 · 위변조 및 OSA(Open Service Access) Gateway, 소프트스위치 등 BcN의 중요 시스템에 대한 침해 위협
- 악의적인 제어 메시지 배포를 통한 불법적인 대역폭 사용, 타인의 대역폭 조정 등을 통한 서비스 품질 저해 및 과다 트래픽 발생을 통한 DoS 및 DDoS 공격에 대한 위협
- 이동성이 보장되고 다양한 접속망이 제공되는 환경에서 복수의 접속기술이 통합된 복합단말기를 통한 공격의 역추적 어려움과 다양한 단말로부터의 유해트래픽 유입에 대한 위험 증가
- 인터넷 침해사고에 취약한 인터넷망에서 발생된 위협이 BcN을 통해 통신망, 방송망 및 USN까지 확산 가능

이와 같이 정보통신망 기능의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 제반 위협과 부작용 등의 정보화 역기능에 대한 대응을 위하여 BcN 정보보호가 필요하다. BcN에서는 이기종 망간 통합 및 여러 사업자간에 연동이 이루어지기 때문에 체계적으로 침해사고에 대처하기 위하여 통합 정보보호 관리체계의 구축이 필요하고, 사이버 공격이 갈수록 지능화 · 다양화 · 고속화되는 상황에서 개별망의 피해가 다른 망으로 확산될 수 있는 환경에 대응할 수 있도록 침해사고 예방 및 대응체계에 대한 고도화가 필요하다. 아울러 사용자 프라이버스 보호를 위한 사전 진단 및 지침에 대한 마련이 필요하고, BcN 환경에서 사용될 수 있는 고성능/QoS-aware 네트워크 정보보호 기술이 개발되어야 한다. 또한 정보보호 안정성이 검증되지 않은 VoIP, 텔레매틱스 등 신규 서비스와 다양한 복합단말기에 대한 정보보호 기술이 개발되어야 하고, 신규 IT 서비스의 안정성 확보를 위한 정책적인 지원도 필요하다.

III. MPLS 통신망[5]

MPLS는 전통적인 IP로써는 제공할 수 없는 새로운 서비스와 함께 기존 IP 네트워크의 확장성과 성능을 개선하기 위하여 개발되었다. MPLS는 고속 하드웨어 교환과 QoS 같은 계층 2 교환의 장점을 가지고 계층 3 IP 네트워크를 제공하기 위하여 설계되었다. 이 계층 2 같은 기능성은 MPLS 망의 입구점에서 통상적인 계층 2와 계층 3 헤더 사이에 라벨(label)을 부착하여 이루어진다.

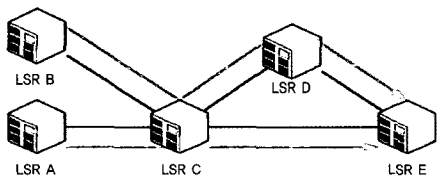
3.1 특성

IP 네트워크는 비연결형 네트워크이기 때문에, 각 라우터는 목적지 주소를 기반으로 수신된 패킷의 다음 홉을 탐색하여 패킷을 전달한다. 그러나 라우터는 가장 긴 접두사 접합(the Longest Prefix Match) 주소 탐색을 사용하기 때문에 고속 패킷 전달을 실현할 수 없다. MPLS에서 전달과정은 전달 테이블을 직접 가리키는 인덱스에 의하여 단순화될 수 있다. MPLS는 패킷 헤더 안에 캡슐화되어 있는 고정 길이의 라벨(label)에 따라서 네트워크 라우팅 제어를 통하여 대역폭 관리를 제공한다. 목적지가 고정-길이 라벨 탐색에 의하여 결정되기 때문에 고속 패킷 전달을 실현할 수 있다. 이 라벨에 의하여 결정되는 패킷 전달 경로를 라벨 교환 경로(LSP: Label Switched Path)라고 한다. 이런 라우팅과 스위칭 기능이 합쳐진 장치를 LSR(Label-Switching Router)이라 한다. 라벨은 이런 두 개의 이웃한 LSR 사이의 가상회선을 나타낸다. 이 라벨은 고속으로 우편물을 처리하기 위하여 우편 서비스에 의하여 사용되는 우편 코드(zip code)와 유사하다.

다른 라벨을 할당함으로써, VoIP(Voice over IP)와 비디오 회의와 같은 애플리케이션에서 지연 증가

에 의하여 나쁜 영향을 받지 않도록 패킷들을 우선적으로 처리할 수 있다. 예를 들어, 지연에 민감한 트래픽을 가진 모든 패킷에 대하여는 보통의 라벨을, 통상적인 데이터를 가진 패킷에 대하여는 다른 라벨을 부착할 수 있다. 그리고 한 조직을 위하여 사용된 라벨들은 같은 서비스 제공자의 다른 고객에 할당된 라벨과는 다르다.

(그림 2)는 MPLS 기반 트래픽 엔지니어링을 보여준다. MPLS는 LSP를 명시적으로 제어하며 해당 트래픽을 위하여 필요한 QoS를 기반으로 최적의 에지-대-에지 경로를 결정한다. 또한 네트워크 내에 각 경로의 부하 분배를 할 수 있는 트래픽 엔지니어링을 제공할 수 있다.



(그림 2) MPLS-기반 트래픽 엔지니어링

3.2 MPLS 설정 정보

MPLS는 IP 패킷의 라벨 교환을 위하여 다음 정보를 사용 한다:

- Forwarding Equivalence Class(FEC): MPLS는 FEC로 같은 전달 처리를 필요로 하는 패킷들의 그룹을 식별한다. 같은 FEC에 속하는 패킷들은 같은 방법으로 처리되며 같은 LSP를 따라서 전달된다. 각 패킷의 FEC는 패킷의 헤더 정보에 의하여 주로 식별된다. FEC는 LSP 종점의 출구 LSR을 통하여 전달될 패킷들의 목적지 주소 접두사의 그룹일 수 있다. 또한 하나의 특정 응용도 IP 주소와 L4 포트 번호에 의하여 식별하는 FEC와 함께 LSP를 따라 단독으로 전달될 수 있다.
- Next Hop Label Forwarding Entry (NHLFE) : 이 정보는 라벨 패킷 전달을 위하여 사용된다. NHLFE는 대치될 다음 홉 라벨 값, 라벨 스택 등을 가진다. 라벨 스택은 다음과 같이 입구 및 출구에서 라벨을 패킷에 부착하거나 삭제하기 위하여 사용된다. 패킷이 특정한 도메인에 들어갔을 때, 입구 LSP는 "라벨 푸시(push)"를 수행하며 패킷에 대한 새로운 라벨을 생성한다. 도메인 내의 연속적인 LSR들은 입력 라벨을 출력 라벨로 변경한다. 패킷이 도메인에 도달되었을 때, 출구 LSR은 "라벨 팝(pop)"을 수행한다.
- 입력 라벨 맵(ILM: Incoming Label Map): 수신된 패킷의 입력 라벨과 NHLFE 사이의 매핑을 위하여 사용된다. 코어 LSR은 수신된 패킷의 입력 라벨을 읽어서 그것의 다음 홉과 ILM을 기반으로 대치될 라벨을 선택한다.
- FEC-대-NHLFE 맵(FTN): 각 FEC와 NHLFE 사이의 매핑을 위하여 사용된다. 에지 LSR은 라벨이 없는 패킷의 FEC를 결정하여 그것의 다음 홉과 FTN을 기반으로 추가될 라벨을 선택한다.

3.3 MPLS 구축 계획

품질보장망으로 고도화하기 위한 기본적인 QoS 서비스 전략은 사업자가 이용자와 SLA(Service Level Agreement)를 체결하고, 이를 기반으로 트래픽 처리 우선순위를 차별화하는 품질보장 서비스를 제공하고, SLA 기반 프리미엄 품질 서비스, 콘텐츠 이용 시마다 요금을 협상하는 QoS 서비스 등을 제공하는 것이다. [1]에서 제시된 단계별 QoS 제공 목표는 <표 1>과 같다.

〈표 1〉 단계별 QoS 제공 목표[1]

단계(년도)	QoS 제공 목표
1단계(2004~2005)	일부 가입자 대상 MPLS 기반 품질보장 서비스 제공
2단계(2006~2007)	MPLS 기반 품질보장망 확대 구축 및 GMPLS 망 도입
3단계(2008~2010)	GMPLS 망 확대, 통합망 관리 등을 통한 End-to-End 품질 보장

IV. QoS 구조의 보안 도입

4.1 QoS 공격 목표

BcN에서 발생할 수 있는 주요한 위협 형태로는 해킹 혹은 침입 공격, 바이러스 및 웜, 서비스 거부, 도청, 위장 공격, 재생 공격, 비인가 접근, 정보 변조, 송수신 부인 등이 있다. 이에 대한 일반적인 대응책으로는 인증, 디지털 서명, 접근 제어, 가상 사설망, 암호화, 침입 탐지 및 방지, 감사 및 기록, 부인방지 등이 있다[6,7]. BcN에서 QoS를 신뢰성 있게 제공하기 위하여 QoS 구조에서 보안 개념이 도입되어야 한다. QoS 공격에 대한 목표는 다음과 같은 것이 있다 :

- QoS 서비스 요구 거부 : 공격자가 예약 메시지의 전부 혹은 일부를 가로채거나 탈락시켜 QoS 예약 및 채널 설정이 지속적인 방법으로 실패하거나 악의적으로 지연될 수 있다.
- 불필요한/suboptimal 자원 예약 : 특정 사용자의 원래 예약 요구와 아주 다른 자원을 공격자가 예약하도록 할 수 있다.
- 네트워크 이용 저하 : 네트워크 시스템이 어떤 QoS 요구사항의 집합을 지원할 수 있을 만큼 충분한 자원을 가지고 있더라도, 네트워크가 작은 부분집합만을 지원하도록 공격자가 예약 프로토콜을 간섭할 수 있다.
- 예약된 QoS 저하 : 어떤 경로를 따라 자원이 성공적으로 예약되고 유지된다고 하드라도, 공격자가 예약된 자원을 비합법적으로 사용할 수 있다. 예약된 자원을 훔침으로써 QoS 저하가 발생할 수 있다.

4.2 문제점

보안은 본질적으로 단일 차원이 아닌 많은 속성들, 즉, 기밀성(confidentiality), 무결성(integrity), 가용성(availability) (CIA)으로 구성되어 있다. 이 세 개의 속성들은 하부 시스템이나 통신 채널들의 다른, 많은 경우 모순된 요구사항을 기술한다. 예를 들어 높은 보안 요구사항을 가진 두 사용자가 각기 다른 요구를 가질 수 있다. 전통적인 보안 해석은 두 가지의 가능한 상태 혹은 값 즉, 안전한가(secure) 아니면 안전하지 않은가(insecure)를 가지고 있다. 그러나 이 이진(binary) 모델로는 불충분하다. 대신에 보안 혹은 그것의 속성들은 하나의 전체 범위의 값을 가지는 척도로 간주되어야 한다[8].

따라서 QoS 구조에 포함될 다른 보안 측면을 위한 정량적인 값에 이르기 위한 방법을 정의하여야 한다. Irvine [9]등은 "변형 보안"(variant security)이라고 하는 개념을 제안하였다. 그들은 보안 메커니즘과 서비스가 보안 범위(security range)를 가지는 것으로 간주하며 그 범위는 적어도 이진(binary)이라는 가정을 하고 있다. 더구나 그들은 여러 가지의 측정 가능한 보안 변수들을 식별하였으며, 이것들이 보안 속성을 간접적으로 정량화하기 위하여 부분적으로 사용될 수 있다. 대부분 기밀성에 대한 보안 변수들에 대하여 조사하였으며, 몇 가지 예는 아래와 같다:

- 암호의 형태(대칭 혹은 비대칭)
- 키와 블록 길이
- 암호화 라운드 수

BcN QoS 구조의 아이디어는 사용자의 필요에 따라서 자신의 품질 레벨을 결정하도록 하자는 것이다. 이와 비슷하게 보안에서도, 사용자에게 이용 가능하

고 구성될 수 있는 속성을 정의하기 위하여 "보안 파라미터"(security parameter)라는 용어를 사용할 수 있다. 보안 파라미터는 보안 변수와 같을 수도 있고 혹은 두개 이상의 결합일 수도 있다. 보안 파라미터에 대한 스케일은 절대적 스케일, 비율(ratio) 스케일, 순서(ordinal) 스케일일 수 있다. 실제 상황에서 "~보다 더 안전한" 관계가 충분할 수 있다[8]. 이와 같은 암호법에 대한 한 가지 예는 다음과 같다:

평문 ≤ DES ≤ AES

이 관계의 해석은 DES(Data Encryption Standard) 암호법으로 인코드 된 메시지는 해당 평문 메시지보다 해독하기 어렵지만, AES(Advanced Encryption Standard)보다는 쉽다는 것이다.

V. MPLS 정보보호

MPLS는 트래픽 분리에 의한 VPN 기능을 제공하기 때문에 보안성에서 장점을 가진다. 그러나 잘못된 구성(mis-configuration)은 MPLS 코어 외부 호스트가 VPN 서비스에 대한 접근을 획득하여 나쁜 영향을 끼칠 수 있다. 본 장에서는 MPLS 정보보호에 대하여 기술한다.

5.1 보안 쟁점

MPLS는 코어를 중심으로 아래와 같은 보안 쟁점들을 기술할 수 있다[10]. 여기서 MPLS 코어는 MPLS VPN 서비스를 제공하는 공급자 에지(PE) 및 공급자 라우터의 집합으로 정의된다[11]. 먼저 코어 외부에서의 보안 쟁점 사항은 아래와 같다.

- 라벨 정보 노출 : 라벨 정보노출로 아래와 같은 이탈 경로 교환 및 이탈 목적지 경로 공격이 발생할 수 있다.
- 이탈 경로 교환 : 만약 트래픽이 의도되지 않은 경로를 따른다면, 이 경로를 이탈 경로(Rogue Path)라고 한다. 만약 공격자가 라벨 정보를 안다면 서비스 제공자의 트래픽 엔지니어링 설정을 우회하도록 만들 수 있다.
- 이탈 목적지 교환 : 공격자가 이탈 목적지로 트래픽을 유도하기 위하여 라벨을 부착할 수 있다. 이렇게 함으로써 서비스 제공자의 트래픽 분리 설정을 피할 수 있고, 예를 들어 원격 익스플로잇 코드에 의하여 생성된 트래픽을 가진 서버에 이르게 할 수 있다.
- 라벨 정보 베이스 중독 : 보통 라벨 분배 프로토콜(LDP: Label Distribution Protocol)이 인증되지 않기 때문에, 코어 외부로부터 LDP 라우팅 정보를 수락하는 경우, 공격자가 라벨 정보 베이스(LIB: Label Information Base)를 조작할 수 있다. 이 기법을 이용하여, 공격자는 DoS와 악성 협조자 공격을 실현할 수 있다.
- 서비스 거부(DoS) : LIB 조작으로 공격자는 DoS 조건을 발생하는 네트워크로 경로를 삽입할 수 있다. 예를 들어, 실시간 요구사항을 가진 트래픽을 혼잡한 경로로 주소를 고쳐 쓸(redirect) 수 있다.
- 악성 협조자 : 만약 공격자가 MPLS 도메인의 LIB를 중독 시킬 수 있다면, 자신의 통제 하에 있는 장치를 해당 도메인의 구성원으로 설정한다. 이 상황을 이용하여 관심 트래픽을 특정 장치로 전달되도록 LIB를 변경할 수 있고, 이 트래픽을 포획하여 나중에 이용을 위하여 저장한다.
- 라벨 에지 라우터로의 비인가된 접속: MPLS 망에 대한 접속을 제공하는 LER(Label Edge Router)이 보안 관점에서 적절히 강화되지 않으면, 비인가된 접속을 통하여 코어 하부구조에 대한 연결 정보 등이 노출될 수 있다.

이외에 라벨 열거(Enumeration of Labels), 라벨 경로 열거, 타깃 열거 등을 제시하고 있다.

코어 내부 장치의 보안 쟁점 사항으로 다음과 같이 기술할 수 있다.

- 일반 IP 트래픽 전달: MPLS 장비가 코어 내부로 라벨 표시가 없는 일반 IP 트래픽을 전달하도록 구성될 수 있다. 이것을 통하여 공격자는 코어 내에서 다른 코어 장치에 이를 수 있다. 트래픽 엔지니어닝과 VPN 능력은 이런 유형의 공격에 보호를 제공하지 못한다.
- 코어에서 외부로 트래픽 전달: 코어 내의 공격자가 LSP를 경유하기 위하여 필요한 라벨을 알면, 트래픽을 코어 외부로 전달할 수 있다.

5.2 요구사항

이 절에서는 MPLS 코어 네트워크는 안전한 방법으로 제공된다고 가정한다. 따라서 비인가된 접속, 코어의 잘못된 구성, 내부 공격 등에 대한 네트워크 요소를 안전하게 하는 기본적인 보안 관심사에 대하여는 기술하지 않는다[7,11,12]. 만일 네트워크가 안전하지 않은 경우, MPLS 하부구조 상에 IPSec을 수행할 필요가 있다. 이 절에서는 MPLS VPN 구조에서 대표적인 보안 요구사항을 기술한다. 그러나 대부분의 경우 일반적인 MPLS에도 적용된다.

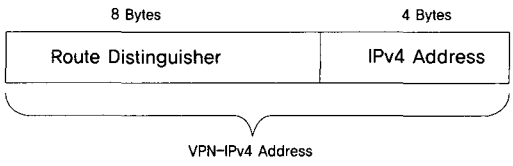
1) 주소 공간, 라우팅 및 트래픽 분리

이 요구사항은 어떤 VPN이 트래픽 분리와 주소 공간 분리에 의하여 다른 VPN이나 코어로부터 별도로 유지되어야 하는 요구사항이다. 좀 더 세부적으로는 다음과 같다.

- 어떤 VPN이라도 다른 VPN과 같은 동일한 주소 공간을 사용할 수 있어야 한다.
- 어떤 VPN이라도 MPLS 코어와 같은 동일한 주소 공간을 사용할 수 있어야 한다.
- 어떤 VPN 트래픽도 다른 VPN으로 가지 말아야 한다.
- 어떤 두 VPN 사이의 라우팅은 독립적이어야 한다.
- 어떤 VPN과 코어 사이의 라우팅은 독립적이어야 한다.

보안 관점에서, 기본적인 요구사항은 어떤 주어진 VPN에서 어떤 호스트로 향하는 패킷이 다른 VPN이나 코어의 동일한 주소를 가진 호스트에 도달하는 상황을 피하는 것이다. 기밀성이 어떤 전송 매체 상의 도청에 대하여 보호를 제공하며, 암호화가 사용될 수 있다.

주소 공간 분리를 위하여 RFC 2547은 VPN-IPv4 혹은 VPN-IPv6 주소 패밀리의 개념을 도입하고 있다[13]. VPN-IPv4 주소는 8-바이트 경로 구분자(RD: route distinguisher) 다음에 오는 4-바이트 IPv4 주소로 구성된다. 그림 3은 VPN-IPv4 주소 구조를 보여준다. 비슷하게 VPN-IPv6 주소는 8-바이트 경로 구분자 다음에 16-바이트 IPv6 주소로 구성된다.



(그림 3) VPN-IPv4 주소 구조

RD의 목적은 전체 IPv4 공간이 다른 상황(예를 들어, VPN 용)에서 사용되도록 하기 위함이다. 주어진 라우터 상에서 한 개의 RD는 VPN 라우팅/전달 인스턴스(VRF : Virtual Routing and Forwarding)를 정의할 수 있으며, 전체 IPv4 주소 공간이 독립적

으로 사용될 수 있다.

2) MPLS 코어 구조의 숨김

MPLS 코어 네트워크의 내부 구조는 외부 네트워크에게 보여서는 안 된다. 예를 들어, 공격자가 만일 코어의 주소를 아는 경우 코어 라우터에 대한 DoS 공격이 훨씬 쉽다. 그러므로 MPLS 코어가 대응되는 계층 2 하부구조처럼 외부 네트워크에게 보이게 하면 안 된다. 그러나 보안이 정보의 숨김에 전적으로 의존해서는 안 된다.

3) 공격에 대한 저항

자원에 대한 비인가된 접근을 제공하는 침입 공격에 대하여 네트워크를 보호하는 기본적인 방법이 두 가지 있다. 첫 번째는 남용될 수 있는 프로토콜을 강화하는 것이고, 두 번째는 네트워크를 가능한 한 접근 가능하게 만들지 않는 것이다. 후자는 패킷 필터링이나 방화벽의 사용과 주소 숨김의 결합에 의하여 이루어진다.

DoS 공격에 대한 한 가지 방법은 또한 패킷 필터링이나 주소 숨김에 의하여 타겟 머신에 도착할 수 없도록 하는 것이다.

4) Label spoofing의 불가능성

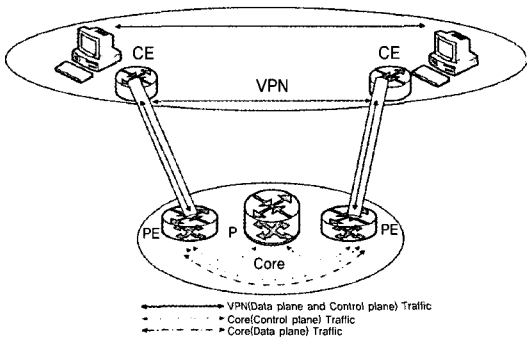
MPLS는 IP 주소 대신에 라벨(label)을 가지고 내부적으로 동작하기 때문에, 이 라벨이 IP 주소처럼 쉽게 속일 수 있는가에 의문이 발생한다. 외부에서 MPLS 네트워크 내부로 PE(Perimeter Edge)를 통하여 외부에서 틀린 라벨을 가진 패킷을 전송하는 것이 불가능해야 한다.

5.3 분석

본 절에서는 앞 절에서 나열된 보안 요구사항 관점에서 MPLS 구조를 분석한다. MPLS는 전통적인 계층 2 VPN 서비스에서처럼 완전한 주소와 라우팅 분리를 제공한다. 코어와 다른 VPN의 주소 구조를 숨기며, MPLS 메커니즘을 남용하여 외부에서 코어로 혹은 다른 VPN으로 침입하는 것이 가능하지 않다. 기밀성이 필요하면 네트워크상에 암호화 서비스를 올림으로써 가능하다. 그러나 MPLS VPN에서 암호화는 표준 서비스가 아니다.

MPLS VPN의 구조로 인하여, 단지 PE 라우터만이 VPN 경로를 알아야 한다. PE 라우터는 VPN 전용으로 VPN-IPv4 주소를 사용하기 때문에 VPN 사이에 주소 공간이 분리된다. 게다가 VPN-IPv4 주소 패밀리와는 다른 주소 패밀리인, 코어 안에서 IPv4를 내부적으로 사용하기 때문에 코어 또한 VPN과는 독립적인 주소 공간을 가진다. 이렇게 함으로써 VPN 간, VPN과 코어 간 분명한 분리를 제공한다.

VPN 트래픽은 VPN 데이터 평면과 제어 평면 트래픽으로 구성된다. 여기서 제어 평면 트래픽은 코어 내부에서 시작하고 종료되는 트래픽이며, 데이터 평면은 여러 VPN으로부터의 트래픽을 포함한다. 이 VPN 트래픽은 보통 LSP 안에서 캡슐화되고 PE에서 PE로 전송된다. 이 캡슐화 때문에 코어는 VPN 트래픽을 볼 수 없다. 그림 4는 MPLS VPN 코어 상에서의 여러 형태의 트래픽을 보여준다.



(그림 4) 트래픽 분리

VPN 트래픽은 VPN 내의 종단 스테이션 사이의 트래픽과 코어 에지(CE: Core Edge) 사이의 트래픽으로 구성된다. 모든 인터페이스는 그 구성에 따라서 단지 하나의 VRF에만 속한다. PE 라우터 상의 분리는 패킷이 라우터에 들어가는 인터페이스의 형태가 non-VRF 혹은 VRF이냐에 따라서 다르게 구현된다. 요약하면 VPN 트래픽 분리는 아래와 같이 실현될 수 있다.

- PE 상의 인터페이스는 하나의 VRF 혹은 코어에만 속할 수 있다.
- 이 인터페이스에 대한 부착 회선(PE-CE 링크)은 사용자의 VPN에 논리적으로 속한다. 다른 VPN은 이곳에 접속을 할 수 없다.
- PE 상에서 VPN의 주소 정보는 모든 VPN을 고유의 경로 구분자(RD)를 통하여 유일하게 만들며, VPN-IPv4 주소로 유지된다.
- VPN 트래픽은 VPN-특정 경로나 터널을 통하여 코어를 통해 전달되며, 이 때 모든 패킷은 VPN-특정 라벨로 보통 태그 된다.
- P 라우터는 VPN을 모르며, VPN 분리와 간섭할 수 없다.

MPLS 코어의 주소 구조를 숨기는 것이 가능하기 때문에, 공격자는 자신이 공격하고자 하는 코어 내의 어떤 라우터의 IP 주소를 모른다. 공격자는 이제 주소를 추측하여 이 주소로 패킷을 전송한다. 그러나 MPLS의 주소 분리로, 각 입력 패킷은 고객의 주소 공간에 속하는 것으로 취급된다. 그리하여 IP 주소 추측을 통하여도 내부 라우터에 도달하는 것이 불가능하다. 이 규칙은 PE 라우터의 피어 인터페이스인 경우에 대하여 단지 예외가 있다.

공격에 대한 저항 능력을 요약하면 다음과 같다. 하나의 VPN으로부터 다른 VPN이나 코어를 침입하는 것은 가능하지 않다. 그러나 PE 라우터에 대하여 DoS 공격을 실행하기 위하여 라우팅 프로토콜을 이용하는 것은 이론적으로 가능하다. 이것이 다른 VPN에 대신 부정적인 영향을 끼칠 수 있다. 그리하여 PE 라우터는 극도의 보안이 요구되며, 특히 CE 라우터에 대한 인터페이스 상에서 그렇다. 라우팅 프로토콜의 포트에 대하여만 그리고 CE 라우터로부터 만 접근을 제한하기 위하여 ACL(Access Control List)이 구성되어야 한다. 라우팅 프로토콜에서의 MD5 인증이 모든 PE/CE 피어링에서 사용되어야 한다. 이러한 잠재적인 DoS 공격의 소스를 추적하는 것이 쉽게 이루어진다.

IP 스푸핑 공격과 유사하게 MPLS 패킷의 라벨을 속이는 것도 이론상 가능하다. 만약 코어 네트워크가 신뢰될 수 없다면 MPLS 망 위에서 IPSec이 수행되어야 한다. 순수한 MPLS VPN 서비스 상에서는 프레임 릴레이나 ATM 네트워크에서처럼 정보 숨김이 유효하다. 만약 VPN 가입자가 인터넷에 접속을 원하는 경우 추가적인 보안 위협에 노출된다. 이 경우 방화벽과 침입탐지시스템과 같은 적절한 보안 메커니즘이 도입되어야 한다.

5.4 보완점

[11,12]에서는 MPLS가 제공하지 못하는 것으로 다음과 같이 기술하고 있다:

- 코어의 잘못된 구성과 코어 내부 공격에 대한 보호

  잘못된 구성의 위험을 피하기 위하여, 장비는 구성하기 쉬어야 한다. 내부 공격의 위험을 피하기 위하여 MPLS 코어 네트워크가 적절히 보호되어야 한다. 이 보안은 네트워크 요소 보안, 관리 보안, 서비스 제공자 인프라의 물리적 보안, 서비스 제공자의 설치에 대한 접근 제어와 다른 표준 서비스 제공자 보안 메커니즘들이 있다.

- 데이터 암호화, 무결성, 기원 인증
  MPLS 자체로는 암호화, 무결성, 인증 서비스를 제공하지 않는다. 이러한 특징이 필요하면, IPSec이 MPLS 인프라 상에 사용되어야 한다 [14].
- 고객 네트워크 보안
  고객 네트워크의 전반적인 보안을 위하여 코어 네트워크의 보안뿐만 아니라 연결의 내외부 및 모든 입구점에서의 보안이 요구된다.

5.5 보안 쟁점에 대한 조치사항

5.5.1 기밀성

LIB와 하부구조를 통과하는 트래픽의 기밀성이 제공되어야 한다. 라벨 값의 전수(brute-force) 열거를 완화하기 위하여, MPLS 하부구조 외부로부터는 라벨 표시된 패킷을 받지 않아야 한다. MPLS VPN은 트래픽 기밀성을 제공하지 않는다. 만약 공격자가 트래픽을 포획하기를 원한다면, 전통적인 IP 네트워크에서처럼 데이터를 읽을 수 있다. 이 문제에 대한 해결책은 암호화 프로토콜을 사용하는 것이며, 대표적인 예는 HTTP 대신에 HTTPS를 사용하거나, 혹은 MPLS VPN 상에 IPSec 터널을 구현하는 것이다.

고객에 의하여 접근될 수 있는 모든 장치와 인터페이스가 보안 관점에서 적절히 강화되어 네트워크 하부구조와 연관된 정보 유출이 최소화되도록 네트워크 운용자는 보장해야 한다.

5.5.2 무결성

MPLS는 LIB를 구축하기 위하여 신뢰된 입력에 의존한다. 이 LIB를 기반으로 전달 결정이 행해진다. LDP 정보와 갱신은 신뢰된 소스로부터 단지 수락되어야 한다. 이것을 위하여 아래와 같은 두 가지 기법이 사용될 수 있다:

- LDP 갱신은 다른 LSR이 위치하고 있다고 알려진 인터페이스로부터 단지 수락될 수 있다. 더 구체적으로 이것은 MPLS 코어 외부의 클라이언트는 LDP 갱신을 할 수 없음을 의미한다.
- MPLS 망 내에 선택된 LDP를 보호하기 위하여 인증 메커니즘이 있어야 한다. 라벨 분배에 사용되는 LDP와 IP 라우팅 프로토콜 BGP는 MD5-기반 인증을 채택하고, 이러한 인증 메커니즘이 라벨 정보의 무결성을 보증하기 위하여 구현되어야 한다.

5.5.3 가용성

악성 협조자가 엉터리 갱신을 통하여 코어 내의 트래픽 플로 주소를 변경할 수 있기 때문에 비인가된 클라이언트로부터의 LDP 갱신을 수락하지 않는 것은 가용성과도 연관이 있다. 이러한 갱신은 MPLS 도메인 내에서 승인된 멤버로부터 단지 수락되어야 한다.

5.6 요약

MPLS VPN은 전통적 계층-2 VPN 서비스에서처럼 완전한 주소 및 트래픽 분리를 제공한다. 코어와 다른 VPN의 주소 구조를 숨기며 MPLS 메커니즘을 오손하여 다른 VPN으로 침입을 할 수 없다. 적절히 보안이 되면 MPLS 코어 내부로 침입하는 것도 불가능하다. 그러나 MPLS의 경우에 코어의 제어 구조가 계층 3이기 때문에 프레임 릴레이나 ATM-기반 VPN과는 상당한 차이가 있다. 이것이 다른 VPN이나 인터넷으로부터 DoS 공격에 대한 가능성을 제공할 수 있다.

본 장에서 기술한 바와 같이, MPLS 인프라의 보안을 해당 ATM이나 프레임 릴레이 서비스 정도로 맞출 수 있다. 또한 MPLS VPN에 대하여 인터넷 연

결성을 안전한 방법으로 제공할 수 있고, 방화벽을 통하여 다른 VPN과 상호 연결도 할 수 있다.

MPLS 코어 내부 공격에 관한한 모든 VPN이 같은 문제를 가지고 있다. 이를 위하여 서비스 제공자는 코어의 보안을 강화하기 위하여 위에서 기술된 여러 가지 예방 조치를 강구해야 한다.

VI. 맺음말

정보통신 인프라에서 보안의 중요성이 빠르게 증가하고 있다. BcN 환경에서는 보안사고 발생시에 그 피해가 전체적인 정보통신 인프라에 보다 빠르게 광범위하게 확산될 수 있기 때문에 더욱 심각한 통신 피해가 우려되고, 따라서 BcN을 위한 보안 대책이 적절히 수립되어야 한다. 이에 따라 우리나라에서도 단계별 보안 기능 고도화 방안에서 안전하고 신뢰성 있는 사이버 네트워크 환경 구축을 목표로 하고 있다 [1,4].

MPLS는 트래픽 분리에 의한 VPN 기능을 제공하기 때문에 보안성에서 장점을 가진다. 본 논문에서는 MPLS VPN이 아래와 같은 특징을 제공할 수 있다는 것을 기술하였다[13]:

- VPN은 주소 및 트래픽 분리가 제공된다.
- 코어는 쉽게 공격될 수 없다.
- VPN 스푸핑이 불가능하다.
- 코어는 VPN 사용자에게는 보이지 않는다.

MPLS VPN은 ATM과 프레임 릴레이와 같은 전통적인 계층 2 VPN과 비교하여 대부분 동등한 보안을 제공한다. 본 논문에서는 BcN에서 QoS를 안전하게 제공하기 위하여 MPLS 망에서의 정보보호 측면에 대하여 기술하였다.

[참 고 문 헌]

[1] 정보통신부 BcN 구축 기본 계획, 한국전산원, 2004년 2월.

[2] 최준균, "통합 전달망 기반의 BcN 전개와 과제", Telecommunication Review, 2004 특집부록, pp90-113, 2004.

[3] 전용희, "BcN 보안 기술 및 표준화 동향", 한국통신학회지 제 23권 제 3호, pp.405-420, 2006년 3월.

[4] 정보통신부 BcN 구축 연동 계획(2. 통합망 정보보호 체계 고도화), 작업문서, 2005년 12월, BcN 보안 소분과.

[5] 전용희, "인터넷 트래픽 엔지니어링과 QoS 제어 기술", 한국통신학회지 제 22권 제 5호, pp.521-535, 2005년 5월.

[6] B. Gamm, B. Howard, O. Paridaens, "Security features required in an NGN", Alcatel Telecommunications Review, pp.129-133, 2nd Quarter 2001.

[7] Ravi Sinha, MPLS-VPN Services and Security, GSEC Practical Ver 1.4b, Option 1, SANS Institute 2003.

[8] Stefan Lindskog, Erland Jonsson, "Introducing Security in QoS Architectures", http://www.ida.his.se/ida/conf/PromoteIT2002/5D3LindskogStefan.pdf.

[9] Evdoxia Spyropoulou, Timothy E. Levin, and Cynthia E. Irvine, Calculating costs for quality of security service, In Proc. of the 16th Annual Computer Security Applications Conference, pp334-343, New Orleans, Louisiana, USA, Dec. 11-15, 2000.

[10] Thorsten Fischer, "MPLS Security Overview", www.irmplc.com/Docs/MPLS.pdf.

[11] M. Behringer, IETF RFC 4381, Analysis of the Security of BGP/MPLS IP Virtual Private Networks(VPNs), Feb. 2006.

[12] Cisco Systems, White Papers, Security of the MPLS Architecture, Cisco Systems Inc.

[13] Richard Froom, Balaji Sivasubramanian and Erum Frahim, CCNP Self-Study: Building Cisco Multilayer Switched Networks, 3rd Edition, Chapter 3: MPLS Security Analysis, Cisco Press, 2006.

[14] SafeNet, Implementing IPSec over an MPLS Network, August 2003. http://www.safenet-inc.com.

전용희

1971년 ~ 1978년 고려대학교 전기전자전파공학부
1985년 ~ 1987년 미국 플로리다공대 대학원 컴퓨터공학과
1987년 ~ 1992년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 ~ 1978년 삼성중공업(주)
1978년 ~ 1985년 한국전력기술(주)
1979년 ~ 1980년 벨기에 벨가톰(Belgatom)
1989년 ~ 1989년 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 ~ 1992년 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992년 ~ 1994년 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 ~ 현재 대구가톨릭대학교 컴퓨터 · 정보통신공학부 교수
2001년 ~ 2003년 동 공과대학장 역임
2004년 ~ 2005년 한국전자통신연구원 정보보호연구단 초빙연구원
관심분야 : 네트워크 보안, 웜 탐지 및 대응 기술, BcN 보안 및 QoS 보장 기술