2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

MPLS 영역에서의 IP 패킷의 Address 번호의 생략을 위한 LER-to-LER

박상준, 박우출, 곽재원, 정순기, 박상래, 이병호
한양대학교 전자통신전파공학과
e-mail:parksang@hymail.hanyang.ac.kr

LER-to-LER for Omission about Address Field Number of IP over MPLS

Sang-Jun Park, Woo-Chool Park, Jae-Won Kwak,
Soon-Gi Jeong, Sang-Rae Park, Byung-Ho Rhee
Division of Electrical and Computer Engineering, Hanyang University.

요 약

오늘날 매우 널리 사용되는 TCP/IP 프로토콜은 많은 보안적 홈을 가지고 있다. 시퀀스 번호를 스푸핑, 소스 번호를 스푸핑, 인증 공격 등 많은 류의 공격이 이런 홈을 통해서 행해지고 있다. 또한 근원적으로 패킷의 TCP헤더 필드의 포트 번호와 IP 헤더 필드의 주소 번호를 분석하여 포트번호와 IP번호를 알아내어 상대방을 공격한다. 이에 상대방으로부터 어드레스 번호를 은닉하거나 생략하여 전송가능하여 상대방이 패킷을 분석하기 어렵게 만들어 TCP/IP 패킷의 정보를 보호하고자 한다. 이에 본 논문은 MPLS 영역에서 IP 패킷의 헤더의 주소 필드 영역을 LER에서 임의의 매핑 변수에 의해 대체함으로써 MPLS 영역에서의 IP 패킷은 IP 주소 번호를 생략할 수 있다. 이에 본 논문에서는 IP 헤더의 Address field를 제거하기위한 LER을 제안하고 LER-to-LER의 메커니즘을 제시한다.

1. 서 론

인터넷이 본격적인 상업망으로 전환되기 시작하면서 급격하게 양적인 팽창을 거듭하고 있으며, 더욱이 멀지 않은 미래에는 정보 통신 기술과 컴퓨터, 지능형 전자 제품들이 보급됨에 따라서 인터넷의 수요가 폭발적으로 증가될 것으로 예상되고 있다. 이에 따른 빠른 전송과 서비스를 만족시키기 위한 포워딩 기술로써 MPLS에 대한 연구가 활발히 진행중이다. MPLS는 IP 패킷의 흐름(flow)을 MPLS 네트워크 상에 미리 정해진 경로를 따라 전달하는 역할을 담당한다.

또한 인터넷 사용층의 증가와 보안의 요구하는 데이터의 증가에 따라 특정 사이트에 침입하는 일이 빈번해지고 이에 따라 보안에 대한 필요성이 대두되고 있다. 즉 인터넷에 접속하고 어떤 서비스를 제공할 때, 그에 대한 보안에 대한 고려도 이제는 매우 중요한 일이 되었다. 우리나라의 인터넷 관련된 보안 사건을 살펴보면, 93년에 서울대 중앙 교육 전산원의 LANd에 침입하여 6대의 워크스테이션의 정보를 지운 침해사건과 당시 HANA망을 운영하던 한국통신 연구센터의 자료를 지운 한국통신연구센터 침해 사건, 94년도의 인천 지역 정보망인 인디텔에 가입한 선배의 아이디를 도용한 홈뱅킹 계좌이체를 시도한 천리안 홈뱅킹 사건, 95년도 2명의 부산지역 해커를 비롯하여 전국 주요 대학의 시스템을 해킹하다 붙잡힌 사건 등

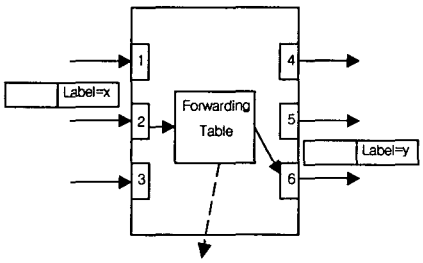
이 한때 간혹 발생하였다. 그러나 오늘날 해킹은 본인이 알게 모르게 하루에 전세계 곳곳에서 빈번히 행해지고 있다.[1,2]

이런 인터넷에서 오늘날 가장 널리 사용되는 TCP/IP 프로토콜은 프로토콜 고유의 여러 가지 흠을 가지고 있다. 이런 결점의 몇몇은 호스트가 TCP의 포트번호나 IP의 어드레스 번호 의지하기 때문에 나타난다. 그래서 본 논문에서는 IP Address를 제거시킬 수 있는 수단으로 MPLS 영역을 통과할 때 레이블을 할당하는 단계에서 LER-to-LER에서 초기에 설정에 의해 Address 번호를 숨기거나 생략하는 방법을 연구하였다. 이런 방법을 통해서 인터넷에서 널리 사용하는 TCP/IP의 패킷을 가로채 분석하는 걸 방지하고자 했다.[3]

본 논문의 구성은 다음과 같다. 2절에서는 MPLS의 라우터의 개략적인 요소와 레이블 분배 방식에 대하여 설명한다. 3절에서는 LER에서 IP 헤더의 주소 필드의 번호를 은닉하는 방법에 대한 LER-to-LER 초기 연결 설정에 대한 메카니즘을 설명한다. 마지막으로 4절에서 결론을 내린다.[3,4]

2. MPLS 개요

MPLS 영역은 다른 망과의 경계 혹은 망의 종단에 위치하여 레이블을 할당하는 동작을 하는 LER과 망 내부에서 레이블 스위칭을 수행하는 LSR로 구성된다. 패킷이 ingress LER로 들어오면 LER은 그 패킷의 헤더의 정보를 모두 분석하여 그에 맞는 FEC로 분류하고 레이블을 할당한다. 이렇게 할당된 레이블을 가지고 MPLS 영영 안의 LSR들은 그 패킷을 전송하고 패킷이 다시 MPLS 영역을 빠져나갈 때 egress LER을 통해 레이블이 제거된 후에 패킷의 헤더의 정보에 따라서 다음 경로로 패킷을 전송한다. 이에 따른 기본 LER의 구조는 그림 1과 같다.



Label IN	Port IN	Label Out	Port Out
x	2	y	6
a	1	m	4

그림 1. Label Swapping as performed by MPLS interior nodes

레이블을 분배하는 protocol을 LDP(Label Distribution Protocol)이라 하고 LDP 기능이 있는 라우터를 LDP peer라 부른다. 이러한 LDP peer 들은 인접한 LDP peer와 메시지를 주고 받아 서로의 레이블 할당의 정보를 교환하고 LIB(Label Information Base)를 구성한다. 이러한 레이블 정보를 가지고 각각의 FEC에 대한 경로를 설정하게 되는데 이 경로를 LSP라 한다. LSP를 따라 레이블 스위칭을 위한 레이블 스와핑은 그림2와 같다.

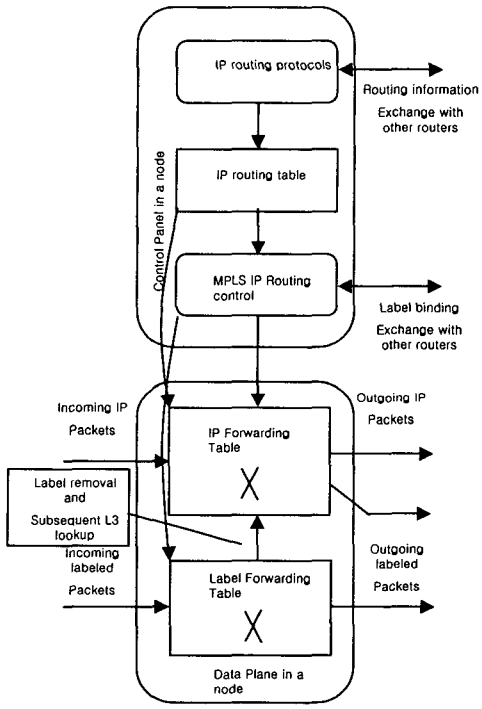


그림 2 Architecture of an Edge-LSR

3. MPLS 영역에서 IP Address Number를 은닉하기 위해 제안된 LER

본 논문에서 제안된 방식은 MPLS 영역으로 진입한 IP 패킷에 대하여 IP 헤더의 Address Number를 은닉하기 위해 LER-to-LER에서 초기 연결 설정에 대하여 수정된 LER 기능에 따른 메카니즘을 제안하였다. 2장에서 언급한 바와 같이 MPLS 영역에서 LER은 LSR 이 레이블 값에 의한 스위칭 기능만을 담당함에 비해서 IP 주소를 검색하고 트래픽을 FEC로 구분하여 LIB에 근거하여 레이블을 할당하는 처리

를 담당한다. 즉 IP 패킷은 MPLS 영역의 ingress LER에 도착하고, 패킷은 LSP에 따라 각각의 LSR에 의해 포워딩된다. 그리고 패킷은 MPLS 영역의 egress LER에 도착하여 레이블을 제거하고 MPLS 영역을 벗어난다. (그림 3)

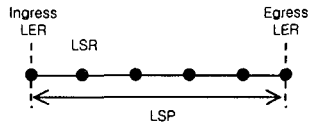


그림 3 MPLS Backbone Network

본 논문에서 제안한 LER-to-LER 의 메카니즘은 그림 4와 같다.

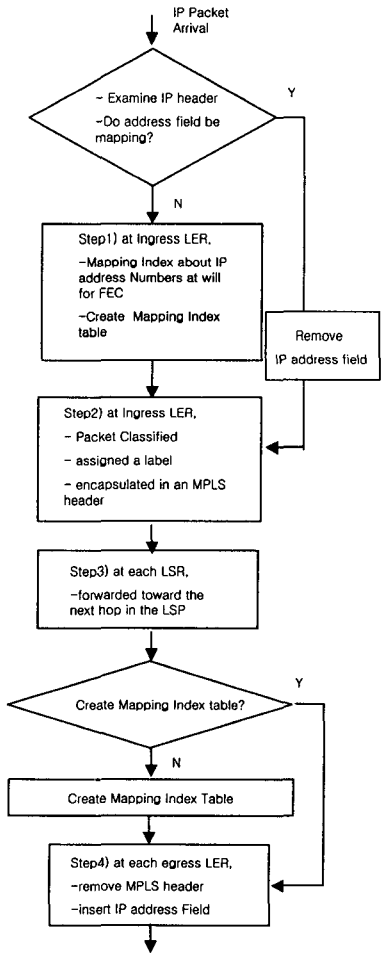


그림 4 LER-to-LER Mechanism

Ingress edge에서 들어오는 패킷의 FEC를 설정하여 첫 번째 IP address field를 조사여 임의의 Mapping Index(MI)로 맵핑하고 그다음에 패킷을 분류하고 레이블을 할당한다음 캡슐화해서 다음 홉으로 포워딩한다. 포워딩된 패킷은 이미 설정된 LSP에 따라 각 홉에서 포워딩되어 egress LER에 도착하여 MI를 설정하고 MPLS 영역을 벗어난다. 벗어날때는 MI를 통해서 IP Address Field를 복구하고 레이블과 MI를 제거하고 MPLS 영역을 벗어난다. 여기서 IP address field를 제거할 때 설정되는 헤더부분의 임의의 Mapping Index를 사용하는 패킷의 헤더내용은 그림 5와 같다.

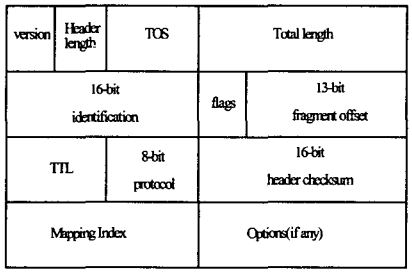


그림 5 제안된 IP Address Field가 제거된 IP 헤더

이처럼 MPLS 영역내를 통해 트래픽을 전달하는 IP 패킷은 IP 주소 부분을 은닉하고 전송함으로써 IP 주소에 대한 정보를 보호할 수 있다.

3 결 론

오늘날 매우 널리 사용되는 TCP/IP 프로토콜은 많은 보안적 홈을 가지고 있다. 시퀀스 번호를 스푸핑, 소스 번호를 스푸핑, 인증 공격 등 많은 류의 공격이 이런 홈을 통해서 행해지고 있다. 또한 근원적으로 패킷의 TCP헤더 필드의 포트 번호와 IP 헤더 필드의 주소 번호를 분석하여 포트번호와 IP번호를 알아내어 상대방을 공격한다. 이에 상대방으로부터 포트번호나 어드레스 번호를 은닉하거나 생략하여 전송하여 상대방이 패킷을 분석하기 어렵게 만들어 TCP/IP 패킷의 보호하고자 한다.먼저 본 논문에서는 IP 헤더의 Address field를 제거하기위한 수정된 LER과 LER-to-LER 연결설정의 메커니즘을 제시하였다.

IP 헤더의 Address field를 제거하여 패킷에 대한 어드레스의 드러남을 방지하여 보안을 강화할 수 있도록 제안된 LER을 사용하여 패킷 전송을 위한 연결이 확립된다.

그 과정에서 첫번째로 옵션 필드에서 레이블 스위칭을 위한 연결 설정이 확립된 후에 소스 주소 필드와 목적지 주소 필드를 대체할 Mapping Index(MI)를 임

의적으로 설정하고 그리고 egress LER 에서는 Mapping Index Table을 만들어 Mapping Index와 주소 필드와 Mapping 상태를 기록하여 IP 주소 필드를 제거할 수 있게 만들어 데이터를 전송할 할 있게 된다. 따라서 그럼으로써 인터넷 망을 통해 전송되는 패킷을 가로채서 IP 주소 정보를 은닉하여 IP 패킷의 보안을 향상시킬 수 있다. 또한 패킷의 양이 감소되는 것을 알 수 있다.

4. 참고 문헌

1. Comer, D. *Internetworking with TCP/IP : Principles, Protocols, and Architecture.* Prentice Hall, 1988

2. Eichin, M. and Rochlis, J. *With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988.* Massachussetts Institute of Technology, 1988

3. S. Floyd and K. Fall, Promoting the Use of End-to-End Congestion Control in the Internet , to appear in IEEE/ACM Transactions on Networking, 1999

4. Awduche, D.O., Malcolm, J., ODELL, M., McManus, J. Requirements for Traffic Engineering over MPLS , draft-ietf-mpls-traffic-eng-00.txt, OCTOBER 1998