MPLS망에서의 보안취약점 분석 및 대응방안

*김도완, 한치문
한국외국어대학교 전자공학과

Threats Analysis and Solution of Security in MPLS Network

Do-wan Kim, Chi-moon Han
Dept. of Electronic Engineering, Hankuk University of Foreign Studies
E-mail : kd0901@san.hufs.ac.kr/cmhan@maincc.hufs.ac.kr

Abstract

This paper describes on the threats in the MPLS Network. Also we discuss on attack scenario that are Unauthenticated Access, Data disclosure and Data modification. Finally we discuss and suggest the best various Security of solutions in MPLS network

I. 서론

최근 정보화의 역기능인 정보유출 및 해킹 등의 보안 사고가 빈번히 발생하고 있다. 이에 대처하기 위한 방식으로 사용자의 시스템 보안은 한계가 있고, 네트워크 자체의 보안이 필요하게 되었다. MPLS망은 현재 인터넷의 문제점인 사용자 및 데이터의 변화와 라우터의 병목현상, 그리고 사용자의 다양한 요구사항을 해결하기 위해 제시된 방식이다. 따라서, MPLS망의 보안 취약점을 분석하고 가장 효율적인 보안 Solution을 제시하고자 한다.

본 논문은 MPLS망에서의 공격 가능한 시나리오를 가정해보고, 여러 방식의 암호알고리즘과 인증 프로토콜을 사용하여, 보안 모델을 구성했다. LDP세션 설정시의 X.509인증 프로토콜 사용, 무결성 제공을 위한 MDC와 MAC방식의 적용과 전송데이터의 기밀성 제공을 위한 암호화방식을 분석하였다. 또한, 인증, 무결성, 기밀성의 제공과 각각의 기능만을 제공하는 모델로 나누고, 보안의 강도를 다르게 정의하여, 이를 바탕으로 전송시간, 데이터의 크기를 시뮬레이션을 통해 측정하여 가장 효율적인 보안 모델을 구현하고자 한다.

II. MPLS망에서의 보안 취약점

2.1 인증되지 않은 단말의 접근

MPLS망에서의 LDP peer discover protocol과 Downstream-on-Demand Label 메시지 사용시에 인증 기능을 제공하지 않으므로 보안상 많은 위협요소가 발생할 수 있다. MPLS의 LDP(Label Distribution Protocol)는 UDP를 이용해서 LDP link hello 메시지를 해당 서브넷의 모든 LSR로 전송하고, 이를 수신한 LSR은 "Hello adjacency"로 응답하여 위치 확인을 한 후, 세션 설정을 할 수 있게 해준다.(직접 연결된 LSR 사이의 경우) 그리고, "Target Hello" 메시지를 통해 직접 연결되어 있지 않은 LSR의 경우에 사용되는데, 지정된 주소의 LSR로 전송하면, 수신한 LSR은 "Hello adjacency"로 응답하여 세션을 설정할 수 있다. 이는 MPLS망 내의 LSR(Label Switching Router)간의 dis

cover를 위한 기능이다.

공격자는 이 기능을 이용해서 자신의 단말을 LSR로 가장하여, Edge-LSR과 MPLS core내의 LSR에 접근한 후, LDP세션 설정이 가능하다. LSR로 가장한 공격자 단말은 Label(ATM의 경우 VCI/VPI값) Request메시지를 통해 LDP peer에게 임의의 FEC의 label 바인딩을 요청할 수 있다.(upstream -> downstream으로 요구) 따라서, 바인딩 값을 얻은 후, 이 값을 조작하여 잘못된 forwarding이 가능하며, 이로 인한 데이터의 유출 및 변조가 일어날 수 있다.

▣ 공격 시나리오

공격자는 LDP 프로토콜을 이용하여, 자신의 단말(Workstation)을 LSR로 위장하는 것이 가능하다.

1) Trace-Router를 이용하여, 각 Router의 IP주소를 획득한다.
2) Edge-LSR까지 ICMP(Internet Control Message Protocol)가 동작하므로, IP주소를 얻을 수 있을 것이다.
3) 각 라우터에게 단계적으로 LDP "Target Hello" 메시지를 보낸다.
4) 메시지를 수신한 Edge-LSR은 "Hello adjacency"로 응답할 것이다.
5) Edge-LSR은 공격자 단말을 LSR로 인식하게 되고, 공격자 단말은 그 다음과정으로 LDP 세션설정을 수행한다.
6) Edge-LSR(In gress/egress)의 IP주소를 확인하면, 그 서브넷 망 내의 모든 IP주소에 "Target Hello" 메시지를 보내서 "Hello adjacency"로 응답이 오는 LSR과의 LDP세션을 설정한다.
7) 공격자 단말은 마치 Edge-LSR과 MPLS core내의 LSR사이에 위치한 LSR로 위장이 가능하게 될 것이다.
8) 공격자는 Label 관리 메시지(Label Request 메시지 등)를 통해 Label 바인딩(VCI/VPI값)을 획득한 후, 이 값을 조작하여, 데이터 경로의 변경 및 정보를 유출시키는 것이 가능하다.

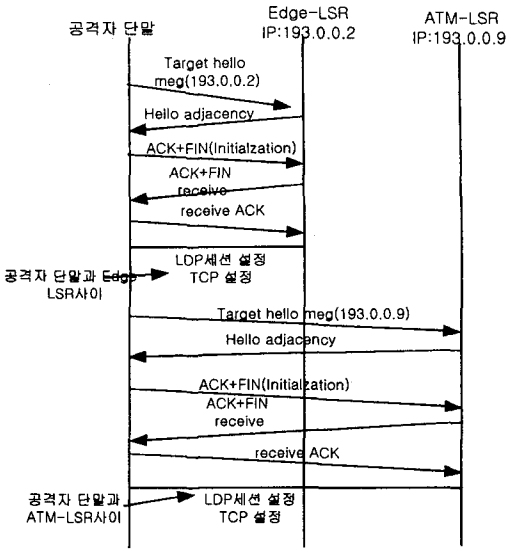

그림 1.공격자가 단말에서 LDP메시지를 이용한 LSR 가장(fake)과정

2.2 정보의 조작

MPLS의 LDP메시지는 세션 설정과 label 관리 기능을 수행하는데, 공격자가 이 메시지를 이용해서 서비스의 중지 및 오동작을 발생하게 할 수 있다. LSR로 가장하여 LDP 세션을 설정한 공격자 단말이 다른 LSR에 조작된 KEEPAlive 메시지,Notification 메시지 등을 생성하여 전송하게 되면, 일반적인 서비스를 수행하지 못할 것이다.

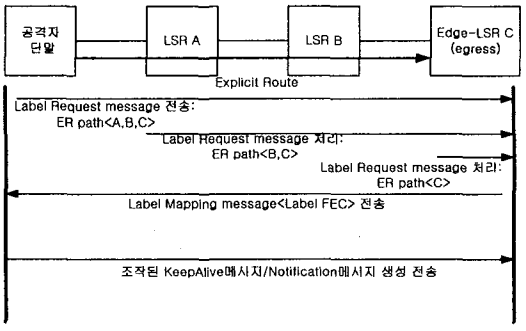

그림 2. LDP 메시지 조작 전송과정

2.3 정보의 유출

LSR로 가장한 공격자 단말이 MPLS의 Label Request 메시지를 Edge-LSR에 보내서 임의의 FEC에 대한 label binding(VPI/VCI)를 요구하여 <Label /FEC>정보를 얻은 후에, Label(VCI/VPI)할당 값을 조작하여 LSP(Label Switched Path)를 변경할 수 있다. 변경된 LSP를 통해 정보가 다른 곳으로 유출이 가능하다.

2.4 서비스 거부(Denial of Service)

MPLS의 Label 바인딩 테이블을 조작하여 공격자 자신의 단말을 통하게 경로 선정을 한 다음, 데이터 패킷내의 TTL(Time to Live)값을 변경하여 망 내의 패킷의 수를 폭주하게 하면 다른 사용자의 서비스를 제공하지 못한다. 그리고, TTL값을 적게 하면, 원래의 목적지로 도착하기 전에 계속 refresh되기 때문에 서비스를 수행하지 못하게 될 것이다. 또한 공격자가 VPI/VCI값을 모두 할당하면 MPLS core내의 이 값을 할당할 수 없게 되어 서비스를 제공할 수 없을 것이다.

III. MPLS(Multi-Protocol Label Switching) 보안 해결방안

3.1 LDP 세션 설정 시 인증 절차 제공

(1) 해쉬 알고리즘 사용으로 무결성 제공

LDP 전체 메시지를 전용 해쉬 알고리즘(MD5)사용하여 나온 이 값(128bit)을 LDP 메시지내의 Optional Parameter 부분에 추가 전송하여 인증되지 않은 공격자가 LDP 메시지를 조작할 경우 이 메시지를 폐기함으로써 무결성을 제공하게 된다.

▣ Data Integrity Algorithm 방식

1) MAC(Message Authentication Code): 키에 기반한 해쉬함수로 무결성 기능만 제공하는 방식이다

2) MDC(Message Digested Code) : 무결성과 인증기능이 포함된 방식이다.

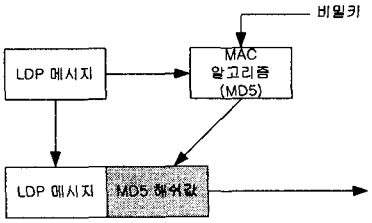

그림3. MAC 방식

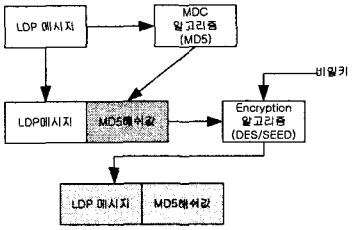

그림4. MDC 방식

(2) 비 대칭키 프로토콜(X.509)의 사용으로 인증(Authentication)기능 제공

LDP세션(TCP) 설정 시에 X.509 프로토콜을 사용하여 인증을 거친 후에, 세션을 설정하게 한다. 따라서, 인증되지 않은 단말의 접근을 막을 수 있게 될 것이다.

▣ X.509프로토콜의 두 가지 방식

Two-pass방식과 Three-pass방식 두 가지를 적용할 수 있다. Two-pass방식은 상호 party간에 동기가 되어 있어야 하며, Three-pass방식은 랜덤 함수를 사용하여 인증 과정을 거친다.

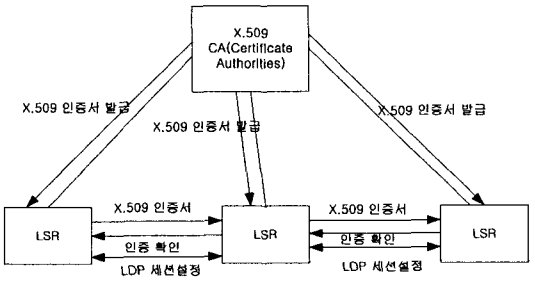

그림5. X.509 프로토콜을 사용한 인증 절차

3.2 전송메시지의 암호화(Encryption)로 기밀성 제공

MPLS에서 전송되는 데이터의 암호화로 기밀성을 제공한다. 따라서 데이터가 유출되어 다른 목적으로 사용되는 것을 막을 수 있다. MPLS - Core내의 전송되는 ATM셀의 암호화 (Triple-DES/SEED 사용)로 전체 전송 속도 저하를 최소화하는 것이 필요하다.

ATM셀의 암호화시에 전송 효율을 위해 2가지 방식으로 암호화를 고려해 볼 수 있다. 먼저 AAL5 PDU의 ATM셀로의 Encapsulation 후에 payload 부분에 암호화할 수 있고, AAL5 PDU의 전체를 암호화한 후, ATM셀로 Encapsulation하는 방안이 있다.

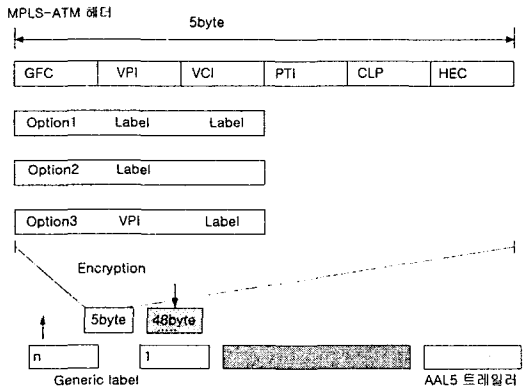

그림 6. AAL5 PDU의 Encapsulation과정

Ⅳ. 최적 보안 모델 구현 및 평가

본 장에서는 앞에서 제시한 보안 Solution을 바탕으로 최적 보안 모델을 제시하였다. LDP세션 설정 시에 X.509 비 대칭키 프로토콜과 Triple-DES MAC를 사용하여 인증기능과 무결성 제공으로 LDP메시지의 조작과 이로 인한 정보의 유출을 막고, MPLS 내의 전송 데이터의 암호화로 기밀성을 제공하였다. 또한, MDC 방식을 사용하여 인증기능과 무결성을 동시에 제공하는 모델을 구현해 보고, MPLS내의 전송데이터의 제공으로 기밀성을 제공하였다.

표1은 보안 위협요소에 대한 보안 Solution 기능에 대한 내용을 나타냈다. 또한, 표2는 Socket 프로그램으로 구현한 전송 효율에 대해 비교하였다.

표1. MPLS망의 Security Scope

Integrity (LDP메시지)	x	○	x	○
Authentication (LDP세션간)	○	x	x	○
Confidentiality (전송데이터)	x	x	○	x

표2. X.509를 적용한 방식과 MDC방식의 비교

	평균전송 처리(Tp)	오버헤드 (DG)	보안 기능
MAC(MD5)	1 Sec	16Byte	Integrity
MDC (Triple-DES)	4.37 Sec	32Byte	Integrity/Authentication
X.509(Triple-DES-MAC)	5.12 Sec	26Byte	Integrity/Authentication
MDC(SEED)	3.53 Sec	32Byte	Integrity/Authentication

Ⅴ. 결론

MPLS망에 대한 보안기능은 기존의 망의 성능 저하를 최소화하는 방식으로 제공되어야 한다. 또한, 유통되는 정보의 중요도에 따라 보안의 강도를 달리 하여 효율적인 보안 기능을 제공해야 한다.

본 논문은 각 보안 기능별로 모델을 구성 비교하여, 이에 따르는 MPLS망의 공격에 대한 대처능력과 각각 시뮬레이션을 통해 전송 시간, 보안 기능의 추가로 발생하는 데이터의 오버헤드를 측정하여 전송효율에 대해 분석하였다. 따라서, MPLS망의 구성 시에 보안 기능을 선택적으로 추가하여 최적화된 보안 모델을 구성할 수 있을 것이다. 향후 실제의 MPLS 망에서 보안 모델의 구현과 효율적인 운영에 대해 연구가 필요할 것이다.

참고문헌

[1] ATM Forum, "ATM Security Specification Version 1.0",af-sec-0100.000, Feb.1999

[2] L.Andersson, P.Doolan ,A.Fredette,B.Thomas LDP Specification, Internet draft<mpls-ldp-07> June 2000

[3] http://www.ietf.org/html.charters/mpls-charter.html

[4] William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY: Principles and Practice