제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

인터넷 라우팅 프로토콜 보안성 진단 연구

김종학*, 문영성*, 김홍철**, 조현철**
*숭실대학교 컴퓨터학부 **국가보안기술연구소
e-mail : mygiant@sunny.soongsil.ac.kr, mun@computing.ssu.ac.kr,
hckim@etri.re.kr, hccho@etri.re.kr

A Study on Internet Routing Protocol Security Vulnerability Diagnosis System

Jonghak Kim*, Youngsong Mun*, Hongchul Kim**, Hyunchul Cho**
*Dept. of Computing, Soongsil University
**National Security Research Institute

요 약

최근 해킹 기술이 다양화되고, 사용하기 손쉬운 해킹 툴들이 개발되고 확산되면서, 라우팅 프로토콜의 취약점을 이용한 해킹 사례 또한 급증하고 있다. 이는 RIP, OSPF, BGP 등의 초기 인터넷 라우팅 프로토콜이 보안에 대한 고려 없이 설계되어서, 이에 대한 간단한 패스워드 및 MD5 인증 등의 보완책으로 등장한 RIPv2, OSPFv2, BGPv4 등도 그 취약성을 계승하고 있기 때문이다. 따라서 현재의 전반적인 라우팅 프로토콜에 문제점을 파악하고, 이를 해결하기 위한 연구가 필요하다. 본 논문에서는 이러한 취약사항들을 이용한 위협 모델들을 분석하고, 이들 위협으로부터 미리 방비할 수 있도록 진단할 수 있는 시스템을 설계 및 구현에 대한 방법을 제시한다.

1. 서론

전자 메일, 월드 와이드 웹, 전자 상거래 등의 수많은 인터넷 서비스들은 물리적인 네트워크 기반에서 TCP/IP 및 OSI 의 표준 프로토콜에 의해 형성된 패킷이 네트워크 사이를 오고 가는 것을 통해서 이루어진다. 이때, 인터넷 같은 규모가 크고 복잡한 네트워크 환경에서 원하는 목적지에 패킷을 제대로 전달하는 것이 라우팅 프로토콜이 하는 일이다.

라우팅 프로토콜은 하나의 단일기관 아래에 있는 라우터와 네트워크 그룹인 AS(Autonomous system)의해 내부 및 외부 라우팅 프로토콜로 구분할 수 있다. 내부 라우팅 프로토콜은 AS 내부에서의 라우팅 정보를 제공하는 프로토콜로 RIP(Routing Information Protocol)과 OSPF(Open Shortest Path First)등이 있고, 외부 라우팅은 AS 사이에서 라우팅 정보를 제공하는 프로토콜로 BGP(Border Gateway Protocol)가 있다.

이들 라우팅 프로토콜은 초기 보안에 대한 고려가 없이 설계되어서 악의의 목적을 가진 사용자에 의해서 라우팅 정보 메시지의 도청 및 조작 등의 위협에 쉽게 노출 될 수 있었다. 그래서 RIPv2, OSPFv2, BGPv4 등의 나중 버전에서는 간단한 패스워드 및 MD5 인증 등의 보완책을 적용함으로써 보안에 대한 부분을 강화하였지만, 지정된 포트사용 및 이전 버전과 함께 동작시 보완책들의 무시 등의 이전 버전이 가지고 있는 취약성을 계승함으로써 여전히 그러한 위협들에 노출되어있다.

이들 위협의 주된 형태는 스프핑과 서비스 거부공격 DoS(Denial of Service)가 될 수 있다. 이들 공격에 의해서 잘못 설정된 라우터나 손상된 라우터는 자신을 통하여 포워딩되는 패킷을 수정하거나 파괴해 버림으로써, 네트워크나 호스트에 도착하지 못하게 할 수 있으며, 또한 패킷을 중간에서 가로채거나 도청할 수도 있다.

본 논문에서는 각 인터넷 라우팅 프로토콜의 보안 취약사항 및 취약사항을 이용한 위협 모델들을 분석함을 통해서, 자신의 망이 노출되어 있는 취약 사항을 진단할 수 있는 보안 취약성 진단 시스템 설계 및 구현 방법에 대하여 제시한다.

2. 인터넷 라우팅 프로토콜들의 보안 취약사항 분석

2.1 RIP/RIPv2 보안 취약사항 분석

RIP 은 홉 개수에 의해서 경로를 결정하는 거리벡터 라우팅을 사용하는 가장 일반적인 내부 라우팅 프로토콜로 사용되지만, 다음 아래 항목들에 의해서 가장 위협하기 쉬운 라우팅 프로토콜로 만든다[1].

첫째, RIP 은 광고 시에 인터페이스의 모든 장비에게 광고하는 브로드 캐스팅 방법 및 전형적으로 UDP 기반의 포트 520 을 사용함으로써 attacker 가 쉽게 라우팅 정보를 수집할 수 있다.

둘째, 내부적인 시퀀스 넘버를 사용하지 않음으로써 오래된 패킷을 되돌리는 형태의 replay 공격으로부터 대비할 수 없다.

셋째, 요청하지 않은 라우팅 광고(unsolicited route advertisements)들을 허용한다. 달리 말하면 조작된 광고나 응답이 수락될 수 있으며, 비록 요청되지 않은 것일지라도 수행하게 된다.

넷째, RIP 데이터는 인증되지 않으며, 암호화를 지원하지 않는다. 이것은 attacker 가 언제든지 RIP 라우터처럼 동작할 수 있거나 라우팅 정보를 조작할 수 있음을 의미한다.

RIPv2 는 간단한 패스워드 사용 및 MD5 해쉬 등의 인증 기능이 추가 되었지만, 거기에는 아래와 같은 몇 가지 한계점을 가지고 있다. [2], [3]

첫째, RFC 2453 에서의 스펙은 단지" clear-text" 형태의 간단한 패스워드 인증만을 지정하였다. 이 방법은 매우 약하며, 쉽게 위협 할 수 있다. 특히, 공유된 패스워드는 RIP 과정에서 명백하게 전송되고, 네트워크 상에서 이 패스워드를 가로챔으로써 취약성을 만들 수 있다. RFC 2082 는 RIPv2 를 위하여 MD5 해쉬를 사용하는 강력한 인증 방법을 정의한다. 그리고 shared key 는 네트워크 상에서 전송되지 않는다. 그러나 이 인증방법은 RIPv2 의 확장 형태로 정의되었고, RFC 2453 에서 제외된 관계로, 범용적 지원에는 무리가 있다. 또한 MD5 해쉬 방법을 사용해도 replay 공격 및 MAC 계산에 의한 취약성은 여전히 존재한다.

둘째, RIPv1 과 함께 동작할 때 인증 과정은 무시되며, 인증의 사용은 명령이 아닌 선택이다.

셋째, 데이터 암호화를 지원하지 않는다.

2.2 OSPF 보안 취약사항 분석

OSPF 는 네트워크 상태에 따라 최단거리를 계산하는 링크 상태 라우팅 방법을 사용하는 가장 많이 사용되는 내부 라우팅 프로토콜로 네트워크를 작은 영역으로 구분하여 계층적으로 구성가능하기 때문에 확장성이 뛰어나다[6],[7].

첫째, OSPF 는 IP 상위 계층으로 TCP 나 UDP 를 사용하지 않고, 새롭게 정의한 프로토콜을 사용하지만, 고정 프로토콜 넘버 89 를 사용하는 것이 정의되어 있다.

둘째, OSPF 의 인증방법은 NULL 인증, 간단한 패스워드 인증, MD5 해쉬 함수 같은 암호학적 인증 등을 사용한다. 이들 인증 방법은 링크의 이웃들 간의 OSPF 메시지들을 인증함으로써, OSPF 지역 내에 조작된 OSPF 메시지를 삽입하는 외부 노드에 대항하는 약간의 보호를 제공한다. 그러나 이 구조는 아래의 2 가지 약점을 가진다. 첫째는 replay 공격에 대한 결점을 가지는 것이다. 둘째는 인증에 대한 문제로 인증을 각 링크 마다 하는 점 및 데이터 암호화 방법 같은 신뢰성을 제공하지 않는 것이다.

2.3 BGP 보안 취약사항 분석

외부 라우팅 프로토콜인 BGP 는 목적지 네트워크를 위한 AS 간의 경로를 순차적으로 기록하는 경로벡터 라우팅을 사용한다. BGP 에서 발생하는 위협들은 아래의 세 가지 기본적인 취약성들에 기인하고 있다 [10~12].

첫째, TCP 포트 179 를 사용함으로써 TCP 의 구조적 취약성을 계승한다.

둘째, RFC 1711 에서는 BGPv4 인증이 지정되었으나, 그러나 적용할 인증 방법에 대해서는 언급하고 있지 않다. RFC 2385 에서는 Cisco 에 의해서 정의된 BGP 의 TCP 세션 계층 아래에서의 MD5 인증을 제공하기 위한 방법 및 랜덤 시퀀스 넘버를 지원함으로써 세션 hijacking 을 어렵게 한다. 그러나 이 인증의 사용은 명령이 아닌 선택이다.

셋째, BGP 의 UPDATE 메시지는 패스 라우팅의 기반이 되는 AS_PATH 필드와 BGP 메시지들이 실제로 광고되는 네트워크를 나타내는 NLRI(Network layer reach-ability information)필드 등은 중요한 역할을 하지만 이들을 지정하는 AS 의 권한 및 신뢰성을 보장하기 위한 메커니즘이 없다.

2.4 HSRP 보안 취약사항 분석

HSRP(Hot Standby Routing Protocol)는 Cisco 에서 구현한 라우팅 프로토콜 기반의 인터넷 프로토콜로 라우터의 집합으로 구성된 HSRP 그룹을 유지하며, 네트워크 상에 호스트의 패킷 포워딩을 기능하는 액티브 라우터가 고장 및 회선 이상에 의해서 패킷을 포워딩 할 수 없을 때, 스탠바이 라우터가 액티브 라우터가 되어서 대신 패킷 포워딩 기능을 할 수 있도록 하며 아래 항목의 취약사항을 가지고 있다[15].

첫째, UDP 기반의 1985 포트를 사용한다.

둘째, 8 바이트의" clear-text" 인증 사용 attacker 에 의해 쉽게 도청 가능하다.

셋째, All Router 멀티캐스트 주소(224.0.0.2) 사용하지만, 대부분의 라우터들이 이 멀티캐스트 주소를 지원하지 않으므로 HSRP 라우터가 속한 LAN 외부로부터의 위협은 어려우나 LAN 에 속한 attacker 로부터 위협이 가능하다.

넷째, HSRP 는 가장 높은" Priority" 를 가진 스탠바이 라우터를 다음 액티브 라우터로 선출하는데, 이러한 구조적 특성을 이용하여 attacker 는 HSRP 메시지의" Priority" 를 조작함으로써 쉽게 액티브 라우터가 될 수 있는 취약점을 가지고 있다.

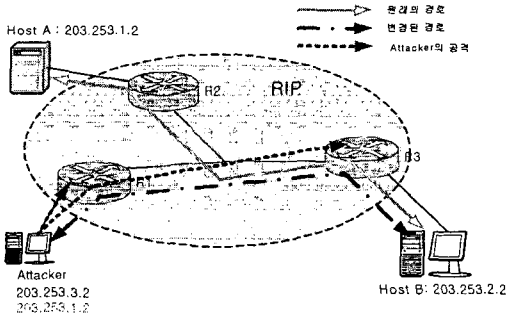
3. 인터넷 라우팅 프로토콜들의 위협 모델 분석

3.1 RIP/RIPv2 의 위협 모델 분석

RIP 에서의 대표적인 위협 모델은 RIP 라우팅 정보 광고 메시지의 스프핑을 이용한 DoS 공격과 Loop 공격으로 볼 수 있다.

예로 DoS 공격을 살펴보면, attacker 가 RIP 라우터로 동작하면서 Host B 의 메시지를 가로채기 위해 조작된 RIP 광고 메시지를 이용하는 형태이다.

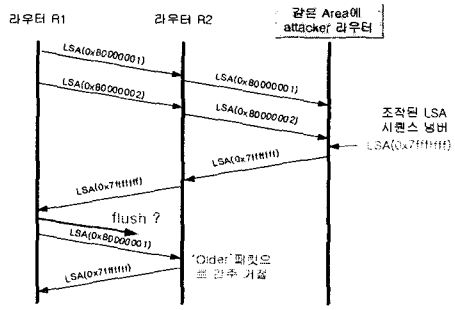
Attacker 는 R1 라우터의" next-hop router" 가 되도록 하고, R1 라우터는 R3 의" next-hop router" 가 되도록 함으로써 Host A 와 Host B 가 정보를 주고 받는 경로를 attacker 의 경로로 수정하여 Host B 가 Host A 와 서비스를 하지 못하도록 할 수 있다.



[그림 1] RIP DoS 모델

3.2 OSPF 의 위협 모델 분석

OSPF 는 엄격한 설정 및 새롭게 정의된 전송층 프로토콜을 사용함으로써 다른 라우팅 프로토콜에 비하여 상대적으로 안정적인 프로토콜이지만, 2 장에서 언급된 취약성을 이용해 여전히 위협 가능하다. 주된 위협 모델로는" Sequence number 가 높은 LSA(Link State Advertisement)를 최근 것으로 판단함" 을 이용하는 Sequence number 위협 및" Age 가 Max age(1 hour)인 것을 최근 것으로 판단함" 을 이용하여 네트워크를 위협이 있다.



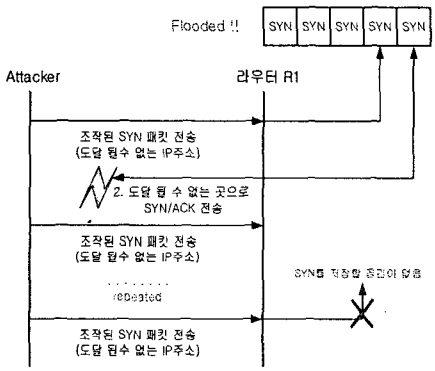
[그림 2] OSPF MAX 시퀀스 위협 모델

[그림 4] 는 Max. Sequence 위협의 예이다. " 현재 가지고 있는 시퀀스 넘버보다 작은 시퀀스 넘버를 가진 LSA 는 수락되지 않음" 을 이용하여 라우터 R1 의 LSA 를 라우터 R2 에서 거절되도록 하는 위협이다.

3.3 BGP 의 위협 모델 분석

BGP 는 TCP 기반에서 동작하는 라우팅 프로토콜로서 주된 위협 형태는 TCP 연결의 취약성을 이용한 SYN Flooding 위협 및 RST DoS 위협 있고, BGP Update 메시지의 취약성을 이용한 스프핑 공격등이 있다.

예로 TCP SYN Flooding 을 살펴보면, attacker 는 R1 에게 도달될 수 없는 IP 주소로 설정된 SYN 를 전송한다. 라우터 R1 은 조작된 SYN 정보를 수신하면 메모리에 저장 후, 이에 대한 ACK 및 SYN 를 도달할 수 없는 곳으로 전송하게 된다. 이때 라우터 R1 은 완전한 연결관계를 위해서는 ACK 가 필요한데, ACK 를 전송 받을 때까지 메모리에 계속 SYN 정보를 유지하게 되어 메모리 자원을 고갈되게 만든다.

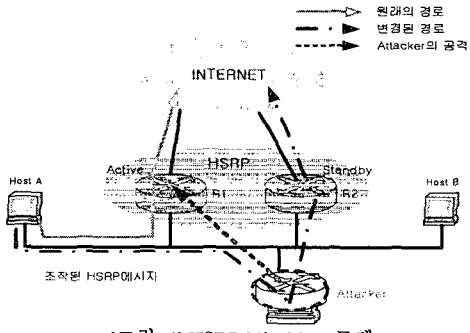


[그림 3] BGP TCP SYN Flooding 모델

3.4 HSRP 의 위협 모델 분석

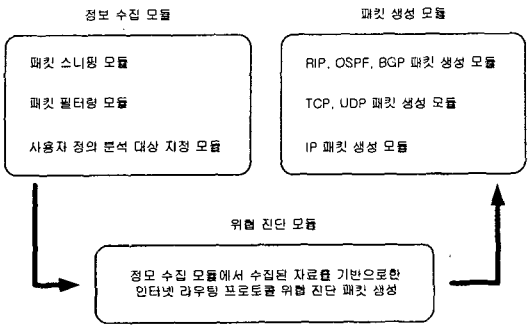
HSRP 에서 주된 위협 모델은 액티브 라우터 선출시에 Priority 에 의존하는 구조적 취약성을 이용한 패킷의 제거, 변경, 도청 유형의 위협이다.

Attacker 는 HSRP 도메인에서 HSRP 기능을 수행 할 수 있는 라우터처럼 동작하면서 액티브 라우터인 R1 에게 자신이 R2 보다 높은 Priority 를 가진 스탠바이 라우터라고 조작된 HSRP 관리 메시지를 보낸다. R1 라우터가 더 이상 Hello 메시지를 광고 하지 않거나 Resign 메시지를 보낼 때 attacker 는 액티브 라우터가 되어 자신을 통해 포워딩되게 되는 Host A 의 패킷들을 위협할 수 있다.



[그림 4] HSRP hijacking 모델

4. 보안 취약성 진단 시스템 구현 방법



[그림 5] 보안 취약성 진단 시스템 구성도

[그림 5]는 인터넷 라우팅 프로토콜 보안 취약성 진단 시스템에 구성도로 상세 설명은 아래와 같다.

- 정보 수집 모듈: 정보 수집모듈은 패킷 스니핑 모듈, 패킷 필터링 모듈 그리고 사용자 정의 분석 대상 지정 모듈로 구성되어 있다. 패킷 스니핑 모듈은 윈도우 기반의 패킷 처리 라이브러리인 winpcap[16]을 이용하여 관련된 모든 패킷들을 수집한다. 수집된 정보들을 기반으로 패킷 필터링을 통한 필요한 정보만 산출한다. 사용자 정의 모듈은 분석 대상 지정을 위한 모듈이다.
- 위협 진단 모듈: 위협 진단 모듈은 정보 수집 모듈에서 수집된 정보를 기반으로 3 장에서 간략히 소개된 시나리오들에 따른 위협 진단을 위한 패킷 정보를 생성한다.
- 패킷 생성 모듈: IETF 표준에 따른 RIPv1, RIPv2, OSPF, BGP 등의 응용 계층 및 TCP, UDP 등의 전송 계층 그리고 IP 계층을 정의 하여 위협 진단 모듈에서 생성된 정보를 적용하여 진단을 위한 라우터들에게 전송한다.

5. 결론 및 향후 연구과제

RIP, OSPF, BGP 등의 초기 인터넷 라우팅 프로토콜은 인증 및 데이터 암호화 등의 보안에 대한 고려 없이 설계되었다. 때문에 악의의 사용자들에 의하여 쉽게 라우팅 정보의 유출 및 절취에 대한 위협에 노출되어있다. 이에 대하여 간단한 패스워드 및 MD5 인증 등의 보완책을 이용한 RIPv2, OSPFv2, BGPv4 등이 등장했지만, 이전 버전과의 상호 동작 및 데이터 암호화를 지원하지 않는 취약성들을 여전히 가지고 있다.

따라서 본 논문에서는 현재의 자신의 네트워크에서 사용하고 있는 라우팅 프로토콜에 대한 문제점을 파악하고, 대처방안을 마련하기 위해서 이를 진단하기 위한 시스템을 구현에 대한 방법을 제시하였다.

향후 연구 과제로는 인터넷 라우팅 프로토콜 취약성을 보완하기 위한 대응방법에 대한 연구 및 라우터 침입 방지 기술에 대하여 연구 하는 것이다.

참고문헌

[1] C. Hedrick, "Routing Information Protocol",. IETF RFC 1058, June 1988.
[2] M. Rose, "RIP version 2", IETF RFC 2082, 1998
[3] G. Malkin, "Routing Information Protocol", IETF RFC 2453
[4] Bradley R. Smith, Shree Murthy, J,J. Garcia-Luna-Aceves, "SECURING DISTANCE-VECTOR ROUTING PROTOLS", IEEE/ISOC Symposiumson Neworks and Distributed System Security, 1996.
[5] J. Etienne, "Flaws in RIPv2 packet's authentication", *IETF draft, 2001*
[6] John Moy, "OSPF Version 2", IETF RFC 2328, April 1998.
[7] S. Murphy, M. Badger, B. Wellington, "OSPF with Digital Signatures", IETF RFC 2154, June 1997
[8] Brain Vetter, Feiyi Wang, S. Felix Wu, "An Experimental Study of Insider Attacks of the OSPF Routing Protocl", In *5th IEEE International Conference on Network Protocols*, Atlanta, GA. IEEE press, October 1997.
[9] Fei-yi Wang, Shytsun F. Wu, "On the Vulnerabilities and Protection of OSPF Routing Protocol", IETF draft, 1998
[10] Y, Rekhter , T. Li, "A Border Gateway Protocol 4(BGP-4)", IETF RFC 1771, March 1995.
[11] Y, Rekhter , T. Li, "A Border Gateway Protocol 4(BGP-4)", IETF RFC 1772, March 1995.
[12] A. Heffernan, "Protection of BGP Sessions via the TCP MD5 Signature Option", IETF RFC 2385, August 1998
[13] Bradley R. Smith, J,J. Garcia-Luna-Aceves, "Securing the Border Gateway Routing Protocol", Proc. Global Internet'96, London, UK, 20-21 Nomember 1996.
[14] http://www.kb.cert.org,"Cisco IOS vulnerable to DoS via unrecognized transitive attribute in BGP UPDATE", Vulnerability Note VU#106392, 10 May 2001
[15] T. Li , B. Cole, P. Morton , D. Li, "Cisco Hot Standby Router Protocol(HSRP)", RFC 2281, March 1998.
[16] winpcap, http://winpcap.polito.it/