악의적인 내부 네트워크 사용을 방지하는 침입 차단 시스템을 위한 패킷 필터링 모듈 설계

이상훈° , 도경화, 정경원, 전문석
숭실대학교 통신연구실
{ iam@leesanghun.pe.kr° khdo0905@dreamwiz.com kwjung09@hanmail.net mjun@computing.ssu.ac.kr }

The model design of packet filtering for Firewall systems with protecting Malicious Usages

Sang-Hun Lee° Kyoung-Hwa Do Kyung-won Jung Moon-Seog Jun
Network Security Lab of Soongsil University

요 약

인터넷의 급속한 발전은 우리 생활의 많은 변화를 가져왔다. 특히 사용상의 편리함과 유용성으로 인해 컴퓨터를 전공하지 않은 사람도 쉽게 접속하여 사용할 수 있게 됨에 따라 악의적인 사용자도 증가하기 시작하였다. 따라서 본문에서는 악의적인 사용자의 접근을 차단할 수 있는 침입 차단 시스템을 설계하고 침입 차단 시스템의 취약점인 TCP Hijacking, IP Spoofing등에도 견딜 수 있는 침입 차단 시스템의 패킷필터링 모듈을 제안한다.

1. 서론

인터넷의 사용자의 꾸준한 증가에 따라 악의적인 사용자 또한 증가하기 시작하였다. 이러한 악의적인 사용자의 접근을 차단하기 위해 침입 차단 시스템의 사용이 일반화되었으나 현재 Man-In-The Middle Attack, TCP Hijacking 그리고 IP Spoofing공격 등 여러 가지 우회방법이 존재한다. 따라서 이를 해결하기 위한 인증 및 다양한 방법의 개발이 이루어지고 있다.

침입차단 시스템은 패킷필터링 및 PROXY, 사용자 인증 등을 통해서 사용자를 인증하고 시스템이나 네트워크에 대한 자원을 사용할 수 있도록 허가 또는 거부한다. 그러나, 이러한 침입 차단 시스템의 방식에 있어서는 인증을 하고 난 후에는 사용자의 접속이 끝난 후를 기다릴 뿐 다른 어떠한 조치를 취하지 않게 된다. 따라서 선의의 사용자가 방화벽에 인증을 받고 난 후 종료하기 전까지가 침입 차단 시스템의 가장 취약한 시기이다.

이러한 취약한 시기에 나타날 수 있는 여러 가지 해킹 기법 중에서 TCP/IP 프로토콜의 취약성을 악용한 공격들이 있다. 이러한 공격들의 일반적인 특징은 정당한 사용자가 합법적인 인증을 받은 후에 서비스 거부 공격(Denial Of Service Attack)이나 사용자의 휴지기간을 이용하여 인증받은 IP로 위조하여 침입 차단 시스템의 인증과 패킷필터링 시스템을 무력화시키는 방법으로 기존 침입 차단 시스템을 우회할 수 있는 수단으로 사용되어 지고 있다.

본 논문에서는 이런 TCP의 보안 취약성 공격 중에서 TCP 하이재킹 공격과 IP 스푸핑 공격이 어떻게 일어나는지 살펴보고 새로운 패킷 필터링 모듈을 제안하여 이러한 공격들에 대처하는 방안을 제시한다.

2. 침입 차단 시스템의 취약점

침입 차단 시스템 패킷 필터링은 관리자가 설정한 정책을 기준으로 하여 네트워크상에서의 패킷의 IP와 비교하여 연결을 허용하거나 거부하는 모듈을 말한다[1]. 그러나 패킷필터링은 이미 연결된 접속에 대해서는 더 이상의 처리를 하지 않는다는 취약점을 가지고 있다. 따라서 이러한 취약점을 중심으로 침입 차단 시스템을 우회하는 다음과 같은 공격들이 존재한다.

2.1 Connection Hijacking Attack

Connection hijacking 공격은 TCP의 스트림을 공격자의 머신을 거치게 리다이렉션 할 수 있는 TCP 프로토콜의 취약성을 이용한 적극적 공격(Active Attack)이다[2]. TCP 하이재킹 공격의 기본적인 아이디어는 해커가 목표 네트웍에 연결하는 컴퓨터의 컨트롤을 얻고, 그 다음 컴퓨터를 네트워크에서 분리시킨 다음에 서버를 속여서 해커가 실제의 호스트의 위치를 차지하는 것이다. 다시 말해, 해커는 신뢰받는 컴퓨터 하이재킹한 다음 목표 컴퓨터로 각 패킷 내의 IP 주소를 해커의 IP주소로 대체하여 전송하므로서 IP를 기반으로 하는 패킷필터링 모듈을 우회할 수 있다.

TCP하이재킹은 공격자가 리다이렉션을 통해서 SKEY와 같은 일회용 패스워드나 커버로스와 같은 티켓 기반 인증 시스템에 의해 제공되는 보호 메커니즘, 그리고 침입 차단 시스템 등을 우회할 수 있다. 그러므로 TCP 접속은 네트워크의 접속로 상에 스니퍼(Sniffer)나 패킷 생성기를 가지고 있다면 대단히 취약하다.

2.2 IP Spoofing

IP 스푸핑 공격은 Spoofing 즉, '속이다'라는 의미이고 IP를 속여서 공격하는 기법을 의미한다. 우선 공격자는 존재하지 않는 IP를 가지고 자신의 IP주소를 위조해 피해 컴퓨터에 SYN를 보내 접속요청을 한다. 요청에 대한 응답으로 피해 컴퓨터가 공격자가 보낸 ACK와 함께 자신의 SYN을 전송하지만 이 주소는 존재하지 않으므로 피해컴퓨터는 자신이 보낸 ACK에 대한 응답을 기다리게 된다. 이 과정을 연속적으로 반복하면 피해 컴퓨터는 외부의 접속요청에 응답할 수 없는 오버플로우 상태가 된다. 이후, 공격자는 패킷 모니터링을 이용하여 관측하고 추측한 순서제어번호를 이용하여 자신의 IP주소를 피해컴퓨터 가장한 후 목표에 접속요청(SYN)을 보낸다. 목표컴퓨터는 수신된 SYN 패킷이 피해

컴퓨터에서 온 것으로 인식, 피해 컴퓨터에게 ACK와 새로운 SYN를 보내지만 이미 피해컴퓨터는 외부와 통신 불능상태이므로 응답을 할 수 없게 된다. 이때 공격자는 자신의 IP 주소를 피해컴퓨터로 위장하여 추측된 순서제어번호를 이용해 B가 A로 보낸 SYN/ACK에 대한 ACK를 목표컴퓨터에 보낸다. 결국 공격자와 목표컴퓨터간의 불법적 접속이 이루어지고, 목표컴퓨터는 피해컴퓨터와 연결되어 있는 것으로 착각한다.

3. 1세대 패킷 필터링 모듈

일반적인 패킷필터링 시스템은 관리자에 의해 설정된 정책에 의해 패킷의 출발지와 목적지 그리고 출발포트와 목적지 포트 등의 정보들로 데이터의 흐름을 허가 또는 거부하는지 결정 할 수 있도록 한다.

그림1과 같은 단순히 규칙에 의해서만 패킷이 필터링 되는 모듈을 "정적 패킷필터링"이라고 한다. 이러한 정적 패킷 필터링은 패킷에 대한 Overhead가 작아 속도가 빠르고 일반적인 네트워크 장비로도 사용할 수 있어 효율적인 장점들을 가지고 있으나 아주 기초적인 검사만 하기 때문에 여러 가지 취약성도 함께 가지고 있다.

그 취약점으로는 외부 클라이언트들에 의한 직접적인 내부 접속이 가능하고 네트워크에 영구적으로 열려 있는 Port를 제공하여야 하며 복잡한 환경에서 빠르게 대처하기가 어렵다. 또한 IP 소스 라우팅[3]에 대한 스푸핑 같은 공격에 취약하다.

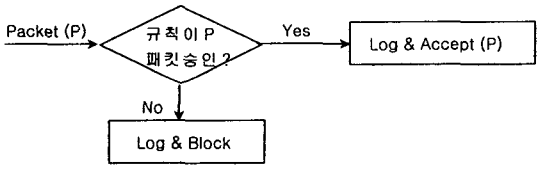

그림 1. 정적 패킷필터링 처리 흐름도

(1) 외부망 및 내부 망에서 패킷이 침입 차단 시스템에 진입
(2) 침입 차단 시스템은 관리자가 세워놓았던 정책에 패킷 P Key(아래부터 Key라 함은 패킷의 Header 정보, Source IP, Source Port, Destination IP, Destination Port[4] 등을 말한다.)를 비교한다.
(3) 정책과 패킷 P가 동일하다면 패킷을 통과시키고 그렇지 않다면 거부한다.

4. 2세대 패킷 필터링 모듈

1세대 정적 패킷 필터링 모듈의 최대의 단점은 네트웍을 사용하기를 원하는 네트웍은 항상 열려 있다는 것이다. 이러한 약점은 전 세계에 네트워크의 취약점을 노출시키는 것과 같다. 예를 들자면 내부에서 나가는 telnet 규칙을 넣는다면 외부에서 내부로 들어오는 규칙도 넣어야 telnet 이 내부에서 외부로의 작동이 되는데 이때 외부에서 내부로의 접근 포트는 항상 열려있어 취약하다는 것이다. 이러한 패킷 필터링 모듈을 개선하기 위해서 2세대 패킷필터링 "동적" 패킷필터링[5]이 개발되었다. 동적 패킷필터링이란 정적 필터링 모듈에 포트를 열고 닫을 수 있도록 하는 것이다. 기본적인 패킷 필터링 기능에 상태 기능을 추가시킨 것으로서 위에서 언급한 사항에 대해서 내부에서 접속을 시도한 패킷이 없다면 외부에서 내부로의 들어오는 연결을 차단시킨다. 이러한 동적 패킷 필터링 시스템은 네트웍 기기에 잠시동안만의 연결을 허용함으로서 네트워크를 항상 Open 시키지 않고 정적 패킷필터링과 비슷한 적은 오버헤드와 빠른 수행능력을 갖는다는 장점이 있으나 정적 패킷 필터링이 가지고 있던 IP 스푸핑등에 의한 공격과 연결 하이재킹에 대한 취약점은 여전히 존재한다.

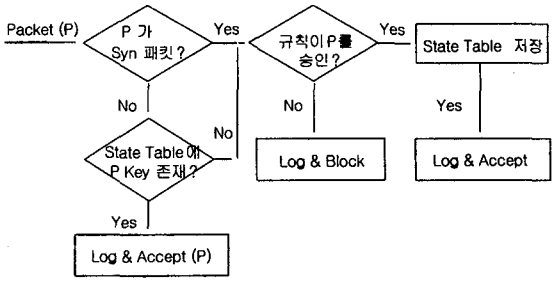

그림 2. 동적 패킷필터링 처리 흐름도

(1) 외부망 및 내부 망에서 패킷이 침입 차단 시스템에 진입
(2) 진입된 패킷 P가 Syn 패킷인지를 확인한 후 Syn 패킷이라면 Rule Table 에 정책이 있는지 확인한다.
  ① 해당되는 정책이 존재한다면 패킷 정보를 State Table에 저장하고 감사기록 후 접속을 허가한다.
  ② Rule Table 에 정책이 존재하지 않는다면 감사기록 후 접속을 차단시킨다.
(3) 진입된 패킷 P가 Syn 패킷이 아니지만 State Table 에 저장된 패킷과 일치한다면 Rule Table과 비교 없이 바로 접속을 허가한다. 만약 일치하지 않는다면 (2)-① ② 과정을 다시 거쳐야 한다.

5. 제안하고자 하는 패킷 필터링 모듈

본 논문이 제안하고자 하는 것은 2세대(동적) 패킷 필터링 모듈에 네트워크 인터페이스 카드의 MAC주소를 정적 매핑 시키거나 동적 매핑시켜 IP 스푸핑, TCP 연결 하이재킹 등의 공격을 막아보자는 데 목적이 있다. 예상되는 기본 환경은 침입 차단 시스템 내부에 공격자가 존재하여 피해시스템의 모든 트래픽을 도청할 수 있는 위치에 있다. 이때 IP 스푸핑과 TCP 연결 하이재킹 등을 이용해서 공격할 수 있는데 두 가지 공격 방식이 접속 전과 접속 후로 나누어 볼 수 있으므로 여기에 대응하여야 한다. 제안하는 패킷 필터링 모듈은 침입 차단 시스템 내부에 있는 공격자가 스니핑을 통하여 이미 연결된 사용자와 침입 차단 시스템간의 네트워크의 연결을 Dos 등을 통하여 공격하고 피해 시스템의 IP주소를 이용하여 방화벽을 우회하려는 시도를 차단하는데 있다. 이는 변경이 불가능한 네트워크 인터페이스의 주소를 침입 차단 시스템에서 관리, 사용하여 공격을 막을 수 있게 하는 것이다. 이러한 방식은 스위치 허브등 네트워크 기기 등을 통하여 시도될 수 있으나 이때는 Switch Jamming, ARP Redirect, ARP spoofing, ICMP Redirect등 여러 가지 해킹 방법이 가능하여 실패할 가능성이 매우 높다. 따라서, 제안하고자 하는 시스템에서 정적 Mapping(고정된 MAC 주소와 IP를 결합하여 침입차단 시스템 관리자로 하여금 정책을 수립)과 동적 Mapping(접속 순간 IP와의 결합을 통하여 시스템에서 자동으로 MAC Table을 관리)을 제안한다.

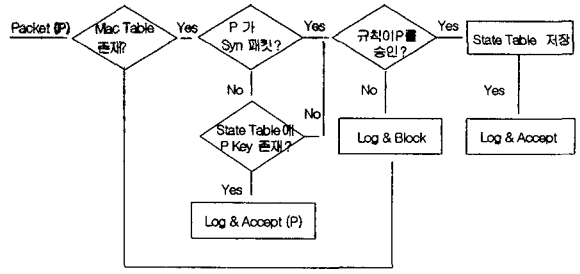

그림 3. 정적 매핑 처리 흐름도

정적 매핑은 관리자가 IP와 MAC주소를 패킷 필터링 정책을 세울 때 미리 기록을 해 주어야 하는 번거로움이 있으나 패킷의 접속 전에 IP와 매핑된 MAC을 확인하기 때문에 외부와의 접속을 성립하기 전 단계에서의 IP 변경의 취약성(IP Spoofing)을 제거 시켜준다[그림3].

(1) 외부망 및 내부 망에서 진입한 패킷인지 확인
   ① 해당되는 정책이 존재한다면 (2) 과정을 수행
   ② Mac Table 에 정책이 존재하지 않는다면 감사기록 후 접속을 차단시킨다.
(2) 진입된 패킷 P가 Syn 패킷인지를 확인한 후 Syn 패킷이라면 Rule Table 에 정책이 있는지 확인한다.
   ① 해당되는 정책이 존재한다면 패킷 정보를 State Table에 저장 후 접속을 허가한다.
   ② Rule Table 에 정책이 존재하지 않는다면 감사기록 후 접속을 차단시킨다.
(3) 진입된 패킷 P가 Syn 패킷이 아니지만 State Table 에 저장된 패킷과 일치한다면 Rule Table과 비교 없이 바로 접속을 허가한다. 만약 일치하지 않는다면 (2)-① ② 과정을 다시 거쳐야 한다.

동적 매핑은 관리자의 정책과는 상관없이 허가를 받은 후 접속한 상태에서의 패킷을 검사하는 것으로서 TCP Connection Hijacking 등에 효율적이다. 이러한 동적 매핑은 침입 차단 시스템의 관리를 편리하게 하며 네트워크 내부의 사용자가 시스템에 있는 네트워크 인터페이스 등을 변경하거나 IP를 변경할 때에도 침입 차단 시스템과는 독립적으로 작업 할 수 있도록 설계되었다[그림4].

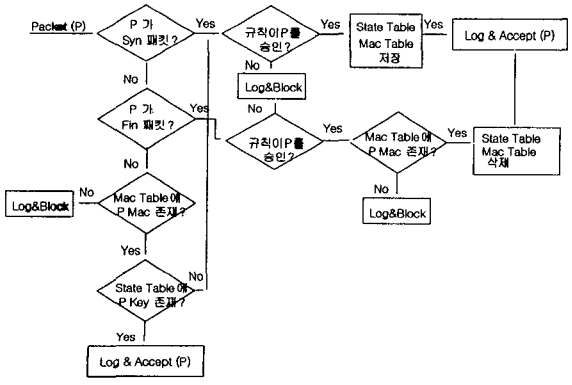

그림 4. 동적 매핑 처리 흐름도

(1) 외부망 및 내부 망에서 패킷이 침입 차단 시스템에 진입
(2) 진입된 패킷 P가 Syn 패킷인지를 확인한 후 Syn 패킷이라면 Rule Table 에 정책이 있는지 확인한다.
   ① 해당되는 정책이 존재한다면 패킷 정보를 State Table에 저장하고 출발지 주소의 Network Interface Card의 MAC 주소를 Mac Table에 기록한 후 접속을 허가한다.
   ② Rule Table 에 정책이 존재하지 않는다면 감사기록 후 접속을 차단시킨다.
(3) 진입된 패킷 P가 Syn 패킷이 아니라면 Mac Table에 진입된 패킷 P와 동일한 Mac 주소를 가진 트래픽이 있었는지 확인한다.
   ① 존재한다면 이러한 패킷은 IP Spoofing 등에 의해서 변조 된 것이 아니므로 (2)의 Rule Table 비교 과정을 수행한다.
   ② 진입된 패킷 P에 대한 MAC 주소와 동일한 MAC table이 없다면 이는 IP Spoofing 등에 의해 IP가 변조된 것이므로 기록을 남기고 접근을 차단한다.
(4) 진입된 패킷 P가 Fin 패킷이라면 정책에 따라 Mac Table에 동일한 Mac Table 이 있음을 확인 후 Mac Table에서 제거한다.

5. 결론 및 향후 연구방향

네트워크의 보안을 생각하면 제일 먼저 떠오르는 것이 침입차단 시스템이며 최근 들어 IDS나 VPN등의 보안기기들과 함께 ESM과 관제 시스템이 등장하고 있다. 그러나 이러한 기기들은 기기의 성능만큼이나 정책이나 설정들이 매우 중요하지만 실제적으로는 잘 설정되지 않고 있다. 따라서 본 논문에서는 패킷 필터링 시스템에 MAC 주소 자동 매핑 기능을 설정하여 관리자의 실수가 반영되지 않고 IP의 변조 유무를 체크할 수 있도록 했다. 하지만 이러한 매핑 자체로서 패킷 필터링의 취약성을 제거할 수 있는 것은 아니다. 앞으로 열려져 있는 포트에 대한 정당한 트래픽과 유해한 트래픽을 자동으로 산출하는 새로운 기술들이 개발되어 패킷 필터링 시스템 모듈을 강화해야할 것이다.

[참고 문헌]

[1] Avolio and Blask. *"Application Gateways and Stateful Inspection : A Brief Note Comparing and Contrasting"*, Trusted Information System, Inc. , pp 1-2. 1998.

[2] Morris, R., *"A Weakness in the 4.2 BSD UNIX TCP/IP Software"*, Computing Science Technical Report NO 117, AT&T Bell Laboratories, 1985

[3] D. Brent Chapman. *"Network (In) Security Through IP Packet Filtering"*, Third USENIX UNIX Security Symposium, September, 1992.

[4] W . Richard Stevens, *"TCP/IP Illustrated , Volume 1: The Protocols"*, Addison-Wesley,1994

[5] Noureldien A.lNoureldien, *"A Stateful Inspection Module Architecture"*, IEEE, pp 259-265, , 2000.