韓國 컴퓨터情報學會 論文誌
第11卷 第2號, 2006. 5.

2006-11-2-4-2

해커의 공격에 대한 지능적 연계 침입방지시스템의 연구

박 대 우*, 임 승 린**

A Study of the Intelligent Connection of Intrusion prevention System against Hacker Attack

Dea-Woo Park*, Seung-in Lim**

요 약

기존의 침입차단시스템과 침입탐지시스템의 단점을 개선할 수 있는 지능적 연계 침입방지시스템을 제안한다. 제안된 보안 시스템은 공격 검출, 공격 우회로 설정 및 통신량 대역 확보, 다른 연계 보안 시스템에 공격 정보 홍보, 내부 IPS에서의 필터 생성, 차단 필터링의 즉각적인 업데이트, 공격 패킷 차단 및 서비스와 포트 차단 설정이다. 스위치 타입 구현과 동적 재설정 메모리들을 통해 새로운 보안 규칙과 패킷 필터링을 실시간으로 교환하고 패킷을 처리한다. 네트워크 성능 실험에서 해커의 공격인 2.5 Gbs의 DDoS, SQL Slammer, Bug bear, Opeserv worm 등에 대한 공격검출이 실시간으로 이루어졌다. 이를 갱신하는 보안 정책 알고리즘의 즉각적인 갱신의 결과로 정상적인 패킷 외에 해커의 공격으로 인한 패킷은 차단되었고, 트래픽은 감소되어, 정상적인 내부와 외부 네트워크 트래픽의 잔여 대역폭을 확보하였다.

Abstract

Proposed security system attacks it, and detect it, and a filter generation, a business to be prompt of interception filtering dates at attack information public information, inner IPS to attack detour setting and a traffic band security, different connection security system, and be attack packet interceptions and service and port interception setting. Exchange new security rule and packet filtering for switch type implementation through dynamic reset memory by real time, and deal with a packet. The attack detection about DDoS, SQL Slammer, Bug bear, Opeserv worm etc. of the 2.5 Gbs which was an attack of a hacker consisted in network performance experiment by real time. Packet by attacks of a hacker was cut off, and ensured the normal inside and external network resources besides the packets which were normal by the results of active renewal.

▸ Keyword : hacker attack, intelligent connection, IPS, information security, virus.

• 제1저자 : 박대우
• 접수일 : 2006.04.12, 심사완료일 : 2006.05.23
* 숭실대학교 정보보안학과, ** 수원과학대학 인터넷정보과

Ⅰ. 서 론

Robert T. Morris의 논문[1]에서 TCP/IP 프로토콜의 취약성이 게재 되었다. Kevin Mitnick[2]은 TCP Syn flooding + TCP Sequence Number Guessing + IP spoof을 사용하여, 모토롤러, 선마이크로시스템즈, NEC, 노벨 등의 컴퓨터 전산망에 침투하여, 소프트웨어 및 각종 자료 등을 훔친 혐의로 1995년 FBI에 의해 체포되었다.

악의적인 의도의 해킹 기법들 중에 Code-Red v2 worm의 출현은 (그림 1)에서 5세대 해킹 컴퓨터 바이러스 모델의 출현을 가속화 시켰다. 불법적인 해커들의 5세대 공격에 대한 완벽한 보안책은 아직 발견되지 않았지만, DoS(Denial of Service)공격[3]이나, DDoS(Distributed DoS) 공격[3]들을 막기 위해 제안된 몇 개의 방법들은 보안 정책에 대한 효과적 결과를 가져 오고 있다.

해커들의 공격에 대한 보안책은 창과 방패의 패러독스와 같아, 해커의 새로운 공격의 형태가 파악되면, 이를 분석하여 공격을 막는 보안책이 개발되는 것이 사실이다. 그러므로 해커의 공격에 대한 보다 적극적인 보안책으로, 해커의 공격을 능동적으로 분석하고 파악하여 지능적으로 연계하는 보안책이 필요하다.

본 논문에서는 이러한 지능적 보안책을 연구하여 컴퓨터 바이러스를 막고, 컴퓨터 네트워크의 보안책으로 지능적 연계 침입방지시스템(ICIPS:Intelligent Connection of Intrusion Prevention System)을 제안한다. 침입방지시스템(IPS:Intrusion Prevention System)[4]은 네트워크의 경계 부분과 게이트웨이 및 내부 네트워크에 위치할 침입방지 보안시스템들로 구성된다. 제안된 시스템은 진화를 거듭하는 악의적인 해커의 공격들이 네트워크 트래픽을 일으키고, 네트워크 컴퓨터 시스템에 침투하는 것을 능동적으로 막는 지능형 보안책을 강구하게 될 것이다.

본 논문은 Ⅰ. 서론에서 연구의 배경과 필요성, Ⅱ. 관련 연구에서의 해커의 5세대, 6세대 공격의 결과 및 분석, Ⅲ. 지능형 연계 침입방지시스템에 대한 적극적인 보안 시스템의 설계, Ⅳ. 지능형 연계 침입방지시스템에 대한 해커의 공격들에 대한 성능 평가, Ⅴ. 결론에서는 제안된 보안 시스템의 평가 결과와 향후 연구로 구성되어 있다.

Ⅱ. 관련연구

본 논문의 연구를 위해 기존의 해커의 공격으로부터 침해를 당한 결과를 통해 세대별로 컴퓨터 바이러스와 해커의 공격 유형별로 구분해 본다. 또한 해커의 최근 5세대에서 6세대 해킹을 중심으로 관련 연구를 하여, 이에 대한 보안책과 보안 시스템을 개발하기 위한 분석 자료로 삼는다.

2.1. 해커와 공격

The New Hacker's Dictionary의 편집자인 Eric Raymond는 '해커(Hacker)'를 솜씨 좋은 프로그래머로 정의하며, 다른 사람의 시스템을 망가뜨리는 사람들이나 또는 악의 있는 행동을 하는 경우는 '크래커(Cracker)'라는 용어를 더 선호한다. 하지만 최근의 대부분 언론과 편집자들은 거의 예외 없이, 해커는 '컴퓨터와 네트워크를 통해 본인의 이익을 추구하거나, 또는 다소 악의적인 목적이나 심지어는 도전이 있다고 생각하면서 컴퓨터 시스템에 침입을 시도하는 사람'으로 정의하고 있다.

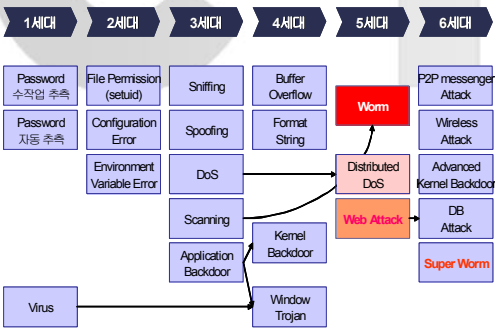

그림 1. 세대별 해커의 공격
Fig. 1. Evolution of Hacker's attack

해커는 컴퓨터와 네트워크를 통해 목표 대상을 공격하기 위해 컴퓨터 바이러스를 만든다. 해커의 공격과 컴퓨터 바이러스를 세대별로 구분해 보면, (그림1)에서 1세대에서는 원시형 바이러스(Primitive Virus)를 이용하고, 패스워드나 ID를 도용하는 것이다. 2세대에서는 암호화 바이러스

(Encryption Virus)를 이용하고, 사용 환경의 허점을 이용하여 침투하였다. 3세대에서는 은폐형 바이러스(Stealth Virus)를 이용하여 네트워크의 취약점을 학습하고, 패킷을 고의적으로 조작하고, 바이러스를 은폐하여 공격 목표 시스템에서의 본인의 이익을 취하려 하였다. 4세대에서는 갑옷형 바이러스(Armour Virus)를 이용하고, 공격자는 시스템에 대한 직접 장애를 유발시키고 네트워크를 다운시켰다. 5세대에서는 웜 바이러스(Worm Virus)를 이용하여, 바이러스 자체가 다른 네트워크와 시스템을 통해 복제되도록 유포시키면서, 공격자의 의도에 의해 대량의 공격을 하도록 하였다. 6세대에서는 진화형 바이러스(Evolution Virus)를 이용하여 P2P환경, 무선 환경 등의 환경 변화에 따라 진화하면서 자기복제와 기술적 진화를 통해, 사안별 공격목표에 따라 적합한 해킹 기술을 조합하여 사용하고 있다.

현재의 해커의 공격은 (그림 1)에서 5세대에서 6세대로 진전되어가고 있으며, Worm공격이나 DDoS 공격들과 같은 악의적인 트래픽을 이용하여 목표 네트워크와 시스템을 공격하고 있다. 또한 해킹기법도 수동 조작 방법에서 자동 조작 방법으로 전환되고 있으며, 인터넷 네트워크 서비스의 가용성에 대한 위협 증대와 유해 트래픽을 폭발적으로 증가시키는 방법을 동원하고 있다. 최근의 초고속 통신 네트워크에서도, 악의적인 인터넷 트래픽은 네트워크 대역폭을 혼잡하게 한다. 컴퓨터 바이러스들은 손쉽게 만들 수 있고, 사용하기 쉬운 공격도구를 통해 해커는 오늘날에도 계속 활동을 하며 사이버 리얼리티(Cyber Reality)[5]에서 활동을 계속 하고 있다.

최근의 피해를 입힌 해커의 공격을 보면 2001년에 새로운 Code Red v2. 웜[6], Nimda Worm[W32/Nimda worm][7], 2002년에 MS SQL 웜[8]와 2003년에 MS-SQL Slammer[8], 2004년에 Phishing[9], 2005년에 웹 게시판 취약점 이용 침입 후 서비스거부 공격[10], 그리고 2006년에 WMF 취약점 관련 악성코드 유포[11] 등의 공격을 통해 전 세계에 걸쳐 심각한 손해를 끼쳤다.

2.2. SYN Flooding 공격

해커는 IP 패킷의 출발지 주소를 위조하여, 존재하지 않거나 도달할 수 없는 주소를 만든다. 그리고 위조된 IP 패킷으로 공격대상 서버에 TCP 커넥션을 통해 연결요청을 하면서 대기 상태를 만들고, 위조된 패킷의 ACK의 전달이 안되어 서버에서 접속확립이 안되게 된다.

결국 공격대상 서버의 큐(queue)에서 접속 내용이 쌓이게 하여, 큐가 가득 차게 되면 정상적인 접속 요구를 못하게 되어 네트워크 서비스를 중지 시키게 한다.

2.3. Code-Red Worm 공격

해커에 의한 Code-Red 공격은 DoS 공격을 발단시킨 계기가 되었다. Code-Red 공격은 해커의 5세대 공격인 Worm을 이용한 해커 공격의 발단이 되었다.

Code-Red Worm의 전파는 Windows 인덱스 서버의 .ida 취약점을 이용하여 확산하였다. 당시 원격 버퍼 오버플로 취약점이 Microsoft IIS web server 버전에 존재한다고 알려졌었다. 해커는 이 취약점을 이용하여 Code-Red Worm을 발생시켰으며, 2001년 7월 12일 Code-Red v1. Worm을 통한 공격을 시작하여, 2001년 7월 19일 Code-Red v2. Worm을 통한 공격으로 전 세계 35만 9천대 이상의 서버가 감염되어, 26억$ 이상의 경제적 손실을 유발시킨 것으로 추정된다[13]. (그림 2)는 Code-Red v2. Worm을 통한 공격을 받았을 때의 화면이다.

그림 2. Code-Red Worm 공격의 증상 화면
Fig. 2. Window in Code-Red Worm

Code-Red v2. Worm을 통한 공격에 대한 피해 상위 10개 국가 별 통계는 (표 1)[13]과 같다.

표 1. 7월 19일 Code-Red v2. 감염 상위 10개 국가
Table. 1. Top 10 countries with Code-Red v2. infected hosts on July 19.

상위 10 개 국가		
국 가	호 스 트	호스트 (%)
미 국	157,694	43.91
한 국	37,948	10.57
중 국	18,141	5.05
대 만	15,124	4.21
캐 나 다	12,469	3.47
영 국	11,918	3.32
독 일	11,762	3.28
호 주	8,587	2.39
일 본	8,282	2.31
네 덜 란 드	7,771	2.16

해커의 5세대 공격인 Code-Red v2 Worm의 공격은 난수 발생의 어려운 점을 해결하여, 보다 강력한 감염 능력의 Worm을 발생하여, Code-Red v1. Worm과 비교하여 6배 이상의 쓰레드(thread)를 발생 시킨 것으로 확인 되었다. 해커에 의한 이 공격은 차후 DDoS 공격과 DRDoS 공격을 할 수 있는 출발점이 되었고, 이후 시스템에 관련한 보안 취약점에 대해 규칙적으로 패치 또는 업데이트 되는 긍정적인 계기를 마련하게 되었다. Code-Red Worm의 공격방법은 다음과 같다.

1) 감염된 시스템은 임의의 IP 주소를 선정한다.
2) 감염된 시스템은 해당 IP 주소로 인덱스 서비스에 버퍼오버플로우를 일으키는 HTTP GET 요구를 보낸다.
3) 만약 공격이 성공하면, c: \network 파일이 있는지 점검한다. 파일이 있으면 활동을 중지한다.
4) c: \network이 없으면, 그 달의 날짜를 기준으로 아래와 같은 주기를 가지고 다른 시스템을 공격한다.
   # 1일 ~ 19일 : 다른 시스템 공격.
   # 20일 ~ 27일 : whitehouse.gov DoS 공격.
   # 28일 ~ 마지막 날 : 휴면(활동 중지).
5) Code-Red Worm 공격은 임의의 IP 주소를 대상으로 공격하기 때문에 한 시스템이 여러 번 공격을 당할 수 있으며, 다른 O.S. 시스템에도 공격 흔적이 남는다. 하지만 다른 O.S.에는 영향이 없다.

Code-Red Worm의 공격과정으로 인한 증상이 나타나면, 시스템 과부하 상태를 점검한다. 감염될 경우 inetinfo.exe의 메모리 사용량이 약 2,000K 정도 증가한다. 간혹 시스템이 다운되는 현상이 발생하기도 한다. 또한 사이트 내에 NT/2000 시스템이 많은 경우, 네트워크 과부하로 인하여 접속이 느려질 수 있다.

2.4. SQL Slammer 공격

해커의 6세대 공격을 유발시킨, 컴퓨터 바이러스에 의한 공격은 SQL Server들을 공격 목표로 하고 있으며 VU#484891 (CAN-2002-0649)[14]에서 기술된 취약점을 이용하여 공격하며, 스스로를 번식 할 수 있다. 이 취약점은 stack buffer overflow가 발생한 후에 무작위 코드가 SQL Server 컴퓨터에 실행되도록 허용한다.

이 바이러스는 2003년 1월 24일에 전 세계의 인터넷을 공격하였다. 그리고 가장 빠른 감염속도를 갖고 있는 바이러스이다. SQL Slammer 바이러스는 공격이 시작된 지 최초 1분 동안에 8.5초마다 두 배씩 증가되었다. 1월 25일 오전 5시 30분 최초 감염 후 10분 안에, Slammer 컴퓨터 바이러스는 전 세계 75,000대 이상의 취약한 호스트를 감염시켰으며, 전 세계의 수천의 다른 호스트들에 대해 잠재적 감염을 시켰을 것이다.

감염된 호스트들은 네트워크를 통해 무수히 많이 복사된 컴퓨터 바이러스를 퍼뜨려 인터넷 트래픽을 통해 통신 속도를 대단히 느리게 하였고, 이 공격으로 인해 인터넷 네트워크에 의존하였던 많은 비지니스 서비스를 방해하였다. 비록 이 컴퓨터 바이러스가 악의적인 내용을 옮기지 않았지만, 이러한 해커의 6세대 공격은 네트워크를 혼란스럽게 하는 원인이 되어 많은 손해를 끼쳤다.

Slammer 크기는 Code-Red Worm 공격과 비교하면, 376byte로 상대적으로 작아서 빨리 복사되는 것이 가능하였다. Code-Red Worm 공격은 크기가 더 커서 상대적으로 천천히 감염되어 퍼졌지만, 잠재적인 피해자들에게 서로 상이한 메시지를 보내 응답을 요구하며, 취약점이 있는 장비들을 공격하여 감염시켰다.

Code-Red Worm 공격은 약 359,000개의 호스트를 감염시켰지만, SQL Slammer 공격은 짧은 시간에 약 75,000개의 호스트를 감염시켰다.

2.5. 변형된 DDoS 공격

해커에 의한 5세대와 6세대의 공격의 특징은 Command 조합과 해킹 Programming에 의한 해킹을 통해 공격자의 신분을 노출 시키지 않는 상태에서 하위 감염시스템을 이용하여 목표를 공격한다.

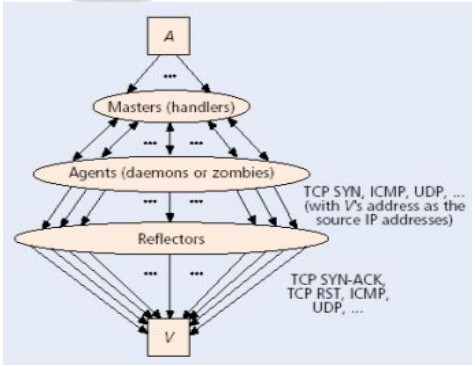

그림 3. DDoS 공격
Fig. 3. Attack of DDoS

(그림 3)처럼 해커인 A는 공격 명령을 통해 배후조종자(Master)를 조종하고, 배후조종자는 대리인(Agent)들을 조

정하고 대리인들은 명령에 따라 종속 호스트(Reflector)들을 조정하여 목표가 되는 서버를 일순간에 공격하여 하여 (그림 4)처럼 폭발적인 트래픽을 유발시켜, 공격 목표 서버가 트래픽을 감당하기 어려워 네트워크 서비스가 중지 되게 한다. 이 공격 모델은 원래 DoS 공격 모델에서 분산된 형태이기 때문에 분산 서비스 거부공격인 DDoS 이라고 부른다.

또한 DDoS 공격은 공격대상 서버로부터 접속 연결 SYN 요청에 대한 응답을 처리하지 않아, 공격하는 호스트들에게 오는 응답을 빗나가게 하여 종속 호스트의 서버가 네트워크 트래픽의 출발지인 것처럼 공격을 한다. 그리고 추적을 하여도 공격자가 노출되지 않는 N:N의 공격을 한다.

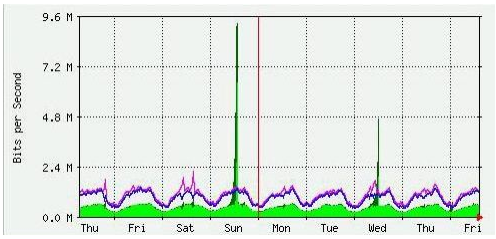

그림 4. DDoS 공격의 트래픽
Fig. 4. Traffics on attack of DDoS

III. 지능적 연계 침입방지 시스템

기존의 내부 네트워크에서 해커의 침입을 차단하는 전통적인 침입차단시스템(Firewall)[15]은 (그림 5)와 같이 서버들의 앞과, 내부 네트워크의 게이트웨이(Gateway)에 위치한다. 침입차단시스템은 외부 네트워크에서 내부 네트워크로 들어오는 패킷을 검사하고, 인증 받지 않는 불법적인 패킷에 대해 차단을 실시한다[16].

(그림 5)에서의 기존의 침입차단시스템은 다음과 같은 단점이 존재한다.

1) 내부 인터넷을 위해 사용이 허가된 서비스 포트(Open-Port)를 경유한 패킷의 침입 방어가 어렵다.
2) 프로토콜의 취약성에 대한 공격, DoS, Worm 등의 동적 공격에 대한 방어책이 없거나 대응이 늦다.
3) 패킷의 헤더만을 조사하며, 페이로드(Payload)는 조사하지 않는다.

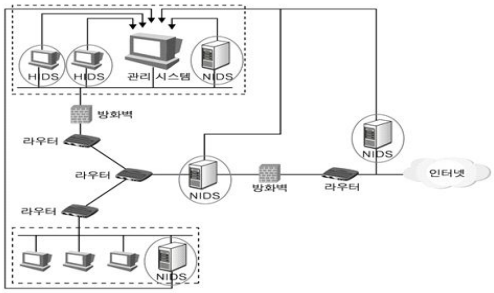

그림 5. 침입차단시스템과 침입탐지시스템
Fig. 5. Firewall & IDS on networks

4) 어필리케이션 레벨(Application Level)의 프락시(Proxy) 서비스는 통신 성능을 저하시켜, 게이트웨이에서의 병목현상을 유발 시킨다.
5) Trojan 방법을 통한 백도어(Backdoor) 등의 우회공격은 차단하지 못한다.

또한 (그림 5)에서 기존의 침입탐지시스템(Intrusion Detection System)은 다음과 같은 단점이 존재한다.

1) 알려지지 않는 공격 패턴에 대해서는 탐지가 어렵다.
2) 짧은 패킷과 비정상 탐지(Anomaly Detection)의 경우 탐지 오판 비율이 높다.
3) 침입 탐지 후에 적극적인 방어 기재가 적다.

이러한 기존 침입차단시스템과 침입탐지시스템의 단점을 극복하기 위해, 본 논문에서 제안하는 지능적 연계 침입방지시스템은 기존의 침입차단시스템 및 침입탐지시스템과 비교하여 다음과 같은 특징들을 목표로 정의한다.

1) 악의적인 트래픽을 유발시키는 DDoS, Worm, Slammer 등의 공격을 적극적으로 방어한다.
2) 서비스 중단이 없는 안전한 보안 알고리즘의 기능 갱신을 실시한다.
3) 해커들의 새로운 공격유형을 지능적으로 파악하고 이를 보안 시스템들과 연계하여 능동적인 차단을 실시한다.
4) 응용 계층(Application Level)의 서비스를 오용과 비정상, 지능적으로 분석하여 탐지하고 이를 침입방지 시스템과 연계하여, 패킷과 서비스 포트를 차단시킨다.

본 논문의 연구는 이런 특징들을 가지고 지능적 연계 침입방지 시스템을 연구한다.

3.1. 지능적 연계 침입방지시스템 설계

지능적 연계 침입방지시스템 구조는 네트워크의 경계에서부터 게이트웨이 및 내부에 위치를 설정하는 것으로 분산된 방어 시스템의 지능적 연계를 제안한다. 해커의 공격으로 인한 악의가 있는 트래픽이 네트워크에 들어가는 것을 막기 위하여 방어 시스템을 재편한다.

지능적 연계 침입방지시스템의 구조는 (그림 6)에서 나타난다. 여기에는 3가지의 특징이 있다. 하나는 악의적인 DDoS나 Worm 공격에 의한 트래픽과 컴퓨터바이러스를 경계 라우터 레벨(Co-Router)과 스위치(Co-Switch)를 이용하여, 침입차단시스템 레벨(Co-Firewall)에서 트래픽 폭주와 해커의 공격을 차단한다.

공격 차단을 위해서는 경계선 라우터가 내부 IPS[17]시스템에 공격 정보를 홍보하고, 내부 침입방지시스템과 연계하여, 해커의 공격을 실시간으로 분석하는 것이다. 분석 결과의 대응책은 실시간으로 발생하는 침입에 대한 방어시스템의 방지 알고리즘이 작동 되면서 보안 규칙 알고리즘들이 설정되고, 악의적인 공격에 대한 이상 징후를 포착하여 침입방지를 즉각적으로 실시하는 것이다.

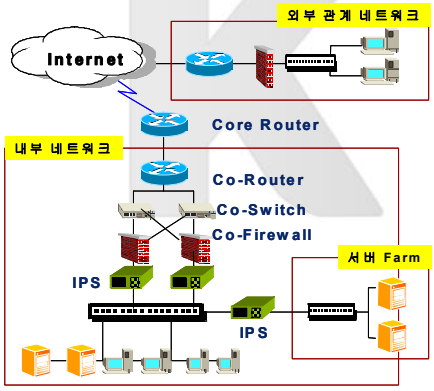

그림 6. 지능적 연계 침입방지시스템의 구조
Fig.6. Architecture of Intelligent Connection IPS.

지능적 연계 침입방지시스템의 제안된 방법은 6단계로 시행된다.

1) 공격 검출

제안하는 방법은 공격 검출은 일차적인 발견된 라우터에서 하며, 지능적 연계 침입방지시스템과 연계된 침입탐지 기능 모듈에서 수행된다. 패킷 계층을 분류하기 위하여 OSI 2-4 Layer의 정보를 사용한다. 공격 검출의 모듈은 기존의 침입차단을 위한 패킷 필터링과 새로 갱신된 공격자의 유형별 공격 패턴과 공격 패킷 정보는 DB에서 분석된 정보를 토대로 하며, 새로운 공격 형태에 관한 것은 IPS에서 통계적 방법을 사용하여 공격을 파악한다.

2) 공격 우회로 설정 및 통신량 대역 확보

공격을 당하는 컴퓨터 바이러스나 웜의 성격에 따라, 평균치 이상의 트래픽이 발생하면, L4나 L7 스위칭 장비를 이용하여 트래픽을 분산 시키면서 공격을 우회시킨다. 우회시킨 공격 패킷들은 내부의 보안 시스템의 보조 메모리 장비를 이용하여 통신량의 대역폭을 확보하여, 네트워크와 시스템 자원의 피해가 가지 않도록 조치된다.

3) 다른 연계 보안 시스템에 공격 정보 홍보

공격 정보는 라우터와 스위칭 장비, 방화벽에 즉시 전송되어 교환된다. 이때 교환정보에 대한 키 기술을 관리하고 있는 연계 침입방지시스템의 네트워크를 사용하여 BGP(Border Gateway Protocol) 과 SNMP(Simple Network Management Protocol)의 확장자를 사용한다.

4) 내부 IPS에서의 필터 생성

내부 IPS에서는 공격 패턴과 침해 사고를 분석하여, 필터를 생성한다. 필터링 규칙은 패킷 분석 후에 즉시 인공 지능적으로 IPS에서 생성되며, 발견되고 분석된 공격 형태, 공격 시간 등과 같은 공격 정보를 위해 필터링과 차단모듈을 홍보하는 제품 속성을 추가한다.

5) 차단 필터링의 즉각적인 업데이트

IPS에 의해 생성된 새로운 필터링 규칙은 라우터의 필터 테이블에 즉시 업데이트 되고 추가된다. 방화벽에서는 필터 테이블과 서비스와 포트 변경에 관한 차단 필터가 업데이트 된다. 인증을 받은 정상적인 패킷에 대한 우회 포트는 능동적으로 설정하게 된다.

6) 공격 패킷 차단 및 서비스와 포트 차단 설정

해커의 공격들은 우선 라우터에 의해 패킷이 차단된다. 게이트웨이의 침입차단시스템은 연계된 내부 침입방지시스템에서 정보를 토대로 패킷과 서비스를 차단한다. 그리고 공격당한 포트도 차단한다.

본 논문에서 제안된 지능적 연계 침입방지시스템은 경계선과 게이트웨이, 내부에서의 악의적인 패킷을 탐지하여 능동적으로 막는 보안시스템의 기능을 갖출 수 있다.

3.2. 공격검출시스템의 설계

네트워크의 트래픽은 표준 패킷과 의심스러운 패킷, 그리고 악의적인 패킷으로 구성되어 있다. 악의적인 패킷은 목표에 도달하면 해로운 행동을 한다. 기존의 침입차단시스템은 패킷의 목적지 주소를 읽어낸다. 목적지 주소가 정해지지 않았거나, 부정한 패킷은 폐기시킨다. 하지만 게이트웨이에 설치된 기존의 침입차단시스템 시스템은 공격자들이 정한 목표인 피해자를 구체적으로 규정하지는 않는다.

Worm과 Slammer 등을 이용한 DDoS 공격과 악의적인 패킷을 단계적으로 검출하기 위해 다중필터의 임무 수행에 관한 제안을 한다.

DDoS 공격의 경우에는 많은 공격자가 목표 서버를 공격한다. 악의적인 패킷은 동일한 목적지 주소를 가지고 있다. 같은 목적지 주소를 가진 트래픽 용량은, 내부 네트워크의 앞단 라우터와 게이트웨이를 통과하면서 급속하게 증가한다. 만약 같은 목적지 주소를 가진 트래픽이 통계적 허용치 이상으로 분석되면, DDoS등의 공격 검출 알고리즘을 사용한다.

또한 컴퓨터바이러스의 목적지 주소는 임의로 만들어지나 감염된 서버가 속한 192.168.1.0/24와 같은 네트워크 번지이다. 이렇게 감염된 2번째 서버는 다수의 컴퓨터바이러스의 복사본을 보내므로 패킷을 통해 감염된 서버의 주소지를 내보낸다. 공격 검출 알고리즘을 통해 따라서 패킷정보를 파악하고, 이 정보를 실시간으로 라우터와 게이트웨이 및 내부 네트워크에 홍보하여 패킷 필터링과 서비스의 차단을 설정할 수 있다.

컴퓨터바이러스를 이용한 공격의 경우에, 감염된 서버는 전체 회선 속도로 다른 호스트들에 컴퓨터바이러스 복사본을 보낸다. 이때, 컴퓨터바이러스는 운영체제의 취약점과 유사한 일반적으로 사용되는 포트 번호를 명시한 프로토콜 구조를 가지고 있다. 예를 들면, SQL Slammer는 UDP 1433번, 1434번 포트를 가지고, Blaster는 TCP 135번 포트를 가지고 있다. 따라서 이와 같은 키워드로서 트래픽의 급속한 증가를 유발하는 공격자의 패킷을 검출 할 수 있다.

3.3 차단 필터 기능 설계

패킷필터링의 규칙을 설정할 수 있는 netfilter, iptables 등의 필터 기능을 수행하는 필터링 모듈을 이용하여 공격자의 패킷과 공격자의 서비스 포트를 차단시킨다. 이러한 차단 기능으로는 TCP 확장, Source-Port, Destination-Port, UDP 확장, LOG, REJECT, RETURN, QUEUE와 기존의 세 개의 체인(입력, 출력, 포워드)외에 새로운 체인을 생성하는 사용자 지정의 체인, NAT(Network Address Translation) 활용, 목적지 주소를 192.168.1.2 이나 192.168.1.3 또는 192.168.1.4로 바꾸는 Round Robin 방식에 의한 부하분산 등을 이용하여 차단 필터의 기능을 설계한다.

3.4 신속한 업데이트 기능 설계

현재의 고속 패킷 처리 기능은 ASICs로 구현되고 있다. 따라서 필터링 정책이나 사용되는 프로토콜 및 공격자의 새로운 정보를 수정을 하거나 업데이트를 하기 위해서는, 하드웨어 회로인 기판이나 칩을 바꾸는 절차가 필요하다.

본 논문에서 제안하는 지능적 연계 침입방지시스템은 새로운 공격이 발견될 때마다 새로운 필터링 규칙과 서비스의 중단 없는 알고리즘이 갱신되어야 하므로 1 Gbs 이상의 트래픽을 위해서는 재설정된 디바이스들을 사용한다.

재설정된 디바이스들을 사용하는 갱신 방법은 2가지를 제안 한다[17]. 하나는 스위치 타입 구현이고, 또 다른 것은 버퍼 타입 구현이다.

스위치 타입 구현은 스위칭 장치들을 사용함으로써 설정을 바꿀 수 있다. 첫 번째 스위칭 장치는 재설정된 디바이스는 주요 설정 메모리를 가지고 있고, 다른 디바이스도 새로 설정된 메모리를 가지고 있다. 이 타입 구현에는 하드웨어 디바이스 볼륨의 2배를 요구한다.

버퍼 타입 구현은 동적 재설정 디바이스들을 사용한다. 버퍼 타입의 디바이스는 몇몇 재설정 메모리들을 가지고 있다. 첫 번째 재설정 메모리는 주요한 구성으로서 기록되고, 두 번째 재설정 메모리는 새로운 설정으로서 기록된다.

이로써 동적으로 재설정 메모리들을 통한 공격 검출과 필터링 규칙의 실시간적 지능적 교환을 할 수 있다. 버퍼 타입은 재설정 동안에 패킷을 저장할 수 있으며, 하드웨어 볼륨보다는 스위치 타입을 요구한다.

Ⅳ. 성능 평가 실험

지능적 연계 침입방지시스템을 기존의 라우터와 게이트웨이의 침입차단시스템 및 내부에 IPS시스템을 설치하고, 제안된 공격 검출과 필터링 정책의 지능적 교환 및 침입방지 기능을 위해, 재설정된 디바이스를 채택하고 성능 실험 시스템을 구축하였다.

4.1 해커의 공격에 대한 성능 실험환경

DDoS, SQL Slammer, Bug bear, Opeserv worm 등 해커의 공격에 대한 지능적 연계 침입방지시스템을 평가하기 위해, (그림 8)에 나타난 실험 네트워크에 코어 라우터와 10Gbs 라우터는 내부 네트워크 앞단의 1Gbs의 서브 라우터들을 통하여 네트워크 트래픽이 들어오고, 100Mbs의 SQL 서버들이 연결되는 네트워크 실험 모델을 가정하였다.

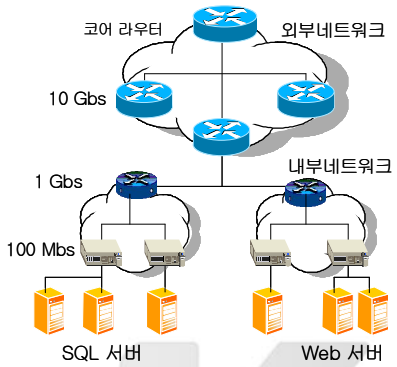

그림 8. 실험 네트워크 모델
Fig. 8. Network Model for Simulation

지능적 연계 침입방지시스템을 검증하도록 사용된 외부 네트워크 시스템은 정상적인 자료 흐름과 DDoS 공격 및 SQL Slammer 컴퓨터바이러스의 전파를 포함한 2.5Gbs 트래픽을 발생시킨다. 성능 실험결과의 수치를 해석하여 정상적 네트워크의 잔여 대역폭을 평가하였다.

모의실험에서 호스트는 '허용', '감염', '이동'의 3개 상태 중 하나의 상태로 가정한다. 시작 단계에서는 외부의 호스트를 임의로 선택하여 최초로 감염 시키고, 다른 호스트들은 모두 '허용' 상태로 전환된다. 감염된 호스트는 임의로 주소가 생성된 다른 호스트에 컴퓨터 바이러스를 복사하여, 전체 회선의 속도로 전파한다. 실험 네트워크의 결과들은 시간과 패킷처리 비율 사이에 관계성을 계산할 수 있다.

제안된 지능적 연계 침입방지시스템의 시작 시간에, 테스트를 위해 침입차단시스템 시스템을 재설정하여 영향을 최소화 하였다. DDoS, SQL Slammer, Bug bear, Opeserv worm 등으로 공격하였으며, 해커의 도구로는 msstream과 Stacheldraht[18]을 이용하여 목표 네트워크와 목표 서버를 공격 하였다. Slammer 바이러스의 패킷 크기는 376바이트로 하였다.

이용 서비스와 사용되는 포트는 IRC(Internet Relay Chat)와 NetBios 네임 서비스는 UDP를 이용한 137번 포트, 서버 메시지는 TCP/UDP을 이용한 445번 포트, MS SQL 서비스는 TCP/UDP을 이용한 1433번과 1434번 포트이다.

지능적 연계 성능의 평가를 위해 각 공격을 1분 단위로 실시한다. 1433번 포트는 사전에 공격에 대한 차단 설정을 하지 않는 상태에서, 능동적인 차단 알고리즘의 갱신이 이루어지지 않은 상태로 실험을 하였고, 1434번 포트의 공격은 외부 라우터와 침입차단시스템을 통해서, 공격차단 알고리즘이 설정된 상태에서 능동적인 차단 알고리즘이 이루어진 상태로 실험을 하였다.

감염 지연 시간은 감염된 호스트에서 이차 감염 호스트로의 이동 시간으로 정의된다. 실험에서는 감염 지연시간을 0.1초로 가정했다. 감염된 호스트는 다른 복제된 컴퓨터바이러스에 의해 재감염 될 경우, 감염행동을 바꾸지 않을 것을 가정한다.

4.2 해커의 공격에 대한 성능 실험 결과

MS SQL Slammer 공격은 사전에 공격에 대한 차단 설정을 하지 않는 상태에서 능동적인 차단 알고리즘의 갱신이 안 이루어진 상태로 1433번 포트를 통해 실험을 하였다. 1434번을 통한 공격은 외부 라우터와 침입차단시스템을 통해서 공격차단 알고리즘이 설정된 상태에서 능동적인 차단 알고리즘이 이루어진 상태로 실험을 하였다.

Opserv 웜과 Bug Bear를 이용하여 (그림 9)의 25초 구간부터 137번 포트의 UDP 공격을 통해 550 Mbyte의 트래픽을 유발시켰다. (그림 9)의 실험 30초 후에는 침입을 방지한 결과를 나타내었다. 그리고 라우터, 침입차단시스템과 IPS로 연결되는 연계 IPS는 (그림 9)의 실험 2분 구간과 3분 구간에서는 능동적인 방어로 침입을 방지한 결과를 나타내었다.

DDoS 공격은 (그림 9)의 40초 구간에서 약 1.3 Gbyte의 대량 네트워크 트래픽을 일으키면서 공격 하였다. 하지만 50초 구간 전에 침입이 차단되었고, 침입 방지 시스템이 작동되어 2분 구간에서는 트래픽 발생률이 줄어들었고, 3분 구간에서는 능동적인 방어로 DDoS의 공격을 막아내어 침입을 방지한 결과가 나타났다.

MS SQL Slammer 공격은 (그림 9)의 25초 구간과 1분 50초 구간, 2분 50초 구간에 나누어서 TCP/UDP을 이용하여 1433번 포트와 1434번 포트를 통해 공격이 실시되었다.

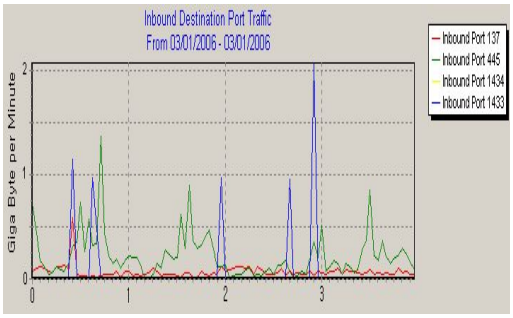

그림 9. 해커 공격의 네트워크 트래픽
Fig.9. Network traffics of hacker's attack

1433번을 통한 공격은 공격 때마다 검출이 되어 차단이 되었지만, 능동적인 차단 알고리즘이 작동하지 않아 (그림 9)의 2분 50초 구간에서 대량의 트래픽의 발생으로 네트워크 대역폭이 줄어들었다. 하지만 1434번 포트에 대한 공격은 외부 라우터와 침입차단시스템을 통해서 공격차단 알고리즘이 작동하여 공격에 대한 차단이 능동적으로 이루어져, 거의 피해를 입지 않는 상태를 나타내었다.

따라서 본 논문에서 Opserv 웜과 Bug Bear를 이용한 공격과 DDoS을 이용한 공격 및 SQL Slammer 컴퓨터바이러스를 통한 해커의 공격에 대한 제안되고 설계된 지능적 연계 침입방지시스템에서의 보안 성능 평가 결과는 우수한 것으로 평가되었다.

V. 결론

이 논문에서 우리는 최근의 해커의 공격 동향인 5세대6세대의 공격방법에 관한 조사와 연구를 하였다. 또한 해커의 공격을 막기 위해 사용되는 기존의 침입차단시스템과 침입탐지시스템의 단점을 살펴보고, 이들을 문제점을 해결하기 위해 본 논문에서 제안된 지능적 연계 침입방지시스템을 6단계인 1) 공격 검출, 2) 공격 우회로 설정 및 통신량 대역 확보, 3) 다른 연계 보안 시스템에 공격 정보 홍보, 4) 내부 IPS에서의 필터 생성, 5) 차단 필터링의 즉각적인 업데이트, 6) 공격 패킷 차단 및 서비스와 포트 차단 설정을 제안하였다.

제안되어 설계된 지능적 연계 침입방지시스템은 재설정이 가능한 프로세스를 사용해 내부 네트워크 앞단의 라우터와 게이트웨이의 침입차단시스템 및 패킷과 서비스를 침입탐지하고 차단 및 방지하는 침입방지시스템은 내부 네트워크에 설치되었다.

침입방지시스템은 내부와 네트워크와 외부 연결 네트워크 시스템의 보안을 위해 설계되었고, 악의적인 컴퓨터바이러스에 대한 트래픽 검출과 10Gbs 유선속도에서의 L4, L7 스위칭 기능을 통한 패킷 처리, 그리고 안정적인 침입차단과 서비스차단을 위한 필터링 알고리즘의 갱신과 기능을 검증하였다.

성능 실험 결과에서 해커의 공격인 DDoS, SQL Slammer, Bug bear, Opeserv worm 등 2.5 Gbs 트래픽을 발생시켰으며, 공격에 대한 지능적 연계 침입방지시스템에서의 공격검출이 실시간으로 이루어졌고, 이를 갱신하는 보안 정책 알고리즘의 즉각적인 갱신의 결과로 정상적인 패킷 외에 해커의 공격으로 인한 패킷은 차단되었고, 트래픽은 감소되어, 정상적인 내부와 외부의 네트워크 트래픽의 잔여 대역폭을 확보하였다. 따라서 지능적 연계 침입방지시스템은 기존의 침입차단 및 침입탐지시스템에 비해 효율적으로 개선되었음을 나타냈다.

향후 연구로는 제안한 부분의 지능적 연결에 대한 프로토콜의 영향 분석과 보안과 필터링 갱신 알고리즘 및 트래픽 배분에 관한 침입방지 기술 연구가 필요하다.

참고문헌

[1] Robert T. Morris. "A weakness in the 4.2BSD Unix TCP/IP software." Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, February 1985.

[2] http://www.webster.edu/philosophy/~umbaugh/courses/frosh/dairy/mitnick.htm, 2006.1.

[3] 박대우, 서정만 "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005.11.30.

[4] McAfee. "White Paper_Host and Network Intrusion Prevention." http://www.mcafee.com/us/local_content/white_papers/wp_host_nip.pdf, February,2005.
[5] 박대우. "멀티미디어 통신망에서의 Cyber Reality의 설계와 구현에 관한 연구." 숭실대학교 석사논문, pp1-84, 1998.8.30.
[6] 보안정보/사고노트/새로운 Code Red II 웜. http://www.krcert.or.kr/index.jsp. 2001.8.5
[7] 보안정보/사고노트/Nimda Worm http://www.krcert.or.kr/index.jsp. 2001.9.19.
[8] 보안정보/사고노트/MS SQL웜 - Spida 분석 및 사고대응. http://www.krcert.or.kr/index.jsp. 2002. 12.8.
[9] 보안정보/사고노트/윈도우즈 시스템 스팸릴레이 사고대책(MS-SQL Slammer). http://www.krcert.or.kr/ index.jsp. 2003.5.13.
[10] 보안정보/사고노트/Phishing Site 사고 분석보고서. http://www.krcert.or.kr/index.jsp. 2004.6.14.
[11] 보안정보/사고노트/웹 게시판 취약점 이용 침입 후 서비스거부공격 사례. http://www.krcert.or.kr/ index.jsp. 2005.8.31.
[12] 보안정보/사고노트/WMF 취약점 관련 악성코드 유포 웹사이트 및 메일서버 분석 사례. http://www. krcert.or.kr/index.jsp. 2006.1.31.
[13] David Moore, Colleen Shannon, Jeffery Brown. "Code-Red: a case study on the spread and victims of an Internet Worm," http://www.caida.org/publications/papers/2002 /codered/codered.pdf
[14] http://nvd.nist.gov/nvd.cfm?cvename=CAN-2002-0649, 2006.1.
[15] 박대우. "무선방화벽의 설계 및 구현에 관한 연구", 한국컴퓨터정보학회논문지, 제8권 제1호, pp44-50, 2003. 3. 31.
[16] 박대우. "접근제어와 사용자인증 프로토콜의 성능개선에 관한 연구." 숭실대학교 박사논문, pp1-122, 2004. 2. 20.
[17] Masaru KATAYAMA, Hidenori KAI, Junichi YOSHIDA, Hiroki YAMADA, Kohei SHIOMOTO, and Naoaki YAMANAKA. "A 10Gb/s Firewall System for Network Security in Photonic Era." IEICE TRANS. Vol. E88-B, No. 5, MAY 2005.
[18] http://www.honeynet.org/papers/enemy/ddos.txt

저 자 소 개

박 대 우

1987년 서울시립대학교 경영학과 졸업 (경영학사)
1995년 숭실대학교 컴퓨터학부 (컴퓨터부전공)
1998년 숭실대학원 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학원 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2003년 숭실대학교 정보과학대학원 정보보안학과 겸임조교수
<관심분야> 유비쿼터스 보안, 시스템 보안, 컴퓨터 및 네트워크 보안, 정보 보안, 이동통신 및 IMT-2000 보안, Cyber Reality

임 승 린

1979년 숭실대학교 컴퓨터학과 졸업(학사)
1987년 숭실대학교 대학원 컴퓨터학과 졸업(석사)
1999년 숭실대학교 대학원 컴퓨터학과 졸업(박사)
1989년 수원과학대학 현재 인터넷정보과 정교수
<관심분야> 응용S/W, 정보시스템, DataBase, 컴퓨터 네트워크 및 인터넷, 지식관리시스템