IPv6 환경에서 SNMP를 이용한 트래픽 폭주공격 탐지

Detection of Traffic Flooding Attack using SNMP on the IPv6 Environment

구향옥, 백순화*, 오창석
충북대학교, 백석대학*

Koo Hyang-Ohk, Baek Soon-Hwa*,
Oh Chang-Suk
Chungbuk National University,
Baeksuk University*

요약

현재 IPv4 환경에서는 서비스 거부 공격과 웜 공격은 피해 규모가 매년 증가하고 있으며, IPv6 환경으로 전환될 때 발생하는 유해 트래픽에 대한 연구가 미약한 상태이다. 본 논문에서는 SNMP(Simple Network Management Protocol)를 이용하여 IPv6 환경에서 예측되는 공격을 수행하여 공격 트래픽을 모니터링하고 공격을 탐지하는 분석 알고리즘을 연구하여 IPv6 환경으로 전환되었을 경우 발생하는 공격을 검출한다.

Abstract

Recently, demage of denial of service attack and worm attack has grown larger and larger every year. But Research of harmful traffic detection is not sufficient when the IPv4 environment is replaced with the IPv6 environment in near future. The purpose of this paper is attact detection which has been detected harmful traffic monitoring on the IPv6 using the Internet management protocol SNMP

I. 서 론

IPv4 주소 고갈 문제로 인하여 IPv6를 테스트하기 위한 망들이 여러 네트워크 환경을 대상으로 시험적으로 도입되고 있다. 국내의 경우 2004년 5월 IPv6 보급 촉진 기본계획통해 국내 환경에 맞는 통신 장비와 서비스를 정부, 학계, 산업체, 연구계 및 사용자와 개발하여 IPv6 주소 사용을 확장하고 있다.

현재 IPv4 환경에서는 서비스 거부 공격과 웜 공격은 피해 규모가 매년 증가하고 있으나, IPv6 환경으로 전환될 때 발생하는 유해 트래픽에 대한 연구는 미약한 상태이다.

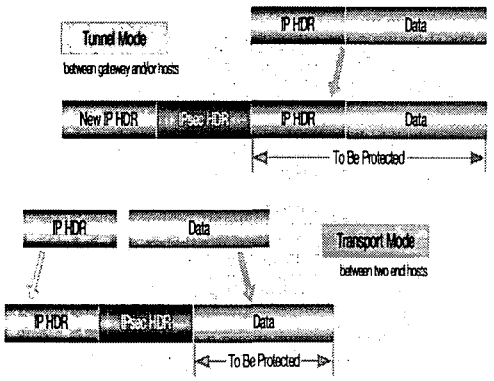
본 연구에서는 IPv6 환경에서 SNMP(Simple Network Management Protocol)를 이용하여 예측되는 공격을 수행하고 공격 트래픽을 모니터링한 다음 공격을 탐지하는 분석 알고리즘을 연구하여 IPv6 환경으로 전환되었을 경우 발생하는 공격 트래픽을 검출한다.

II. IPv6환경 보안

IPv6에서는 기본적으로 IPsec을 사용하여 IP 계층에서의 보호 서비스를 제공함으로써 응용 계층과 독립적인 네트워크로 보안을 가능하게 해준다.

IPsec은 IP 계층에서의 다양한 보호 서비스를 제공하는 것으로 Security Association(SA), Authentication Header(AH), Encapsulation Security Payload

(ESP)의 세 가지 구성요소를 통해 응용 계층과 독립적인 네트워크로 보안이 가능하다. SA는 통신을 시도하는 송수신자간에 미리 정의해 놓은 협약이고, AH는 접근제어(Access Control), 비연결형 무결성(Connnecitonless Integrity), IP 데이터그램에 대한 데이터 발신 인증(Data Origin Authentication)등의 보안 서비스를 제공하며, 선택적으로 재전송 공격방지(Anti-Replay) 서비스를 제공한다. ESP헤더 페이로드에 대해서 AH가 제공하는 서비스 외에 추가적으로 비밀성(Confidentiality) 서비스를 제공하여 각각의 프로토콜은 트랜스포트 모드에서 트랜스포트 세그먼트를 암호화하고, 터널 모드에서는 패킷 전체를 암호화하는 보안기능이 있다.



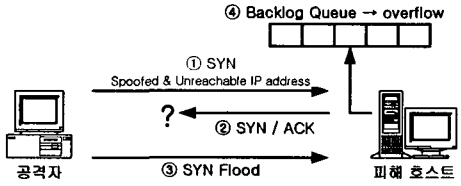
자료출처 : IPv6 Forum Korea

▶▶ 그림 1. IPsec 모드

그러나 IPsec에서 제공하는 보안기능으로는 대량의 트래픽으로 공격해오는 DDoS 등의 트래픽 공격에 대처 할 수가 없다. 이에 본 논문에서는 입력된 트래픽에 대해 TCP, UDP, ICMP 프로토콜 MIB 객체를 분석하여 공격을 검출한다.

1. TCP Flooding 공격

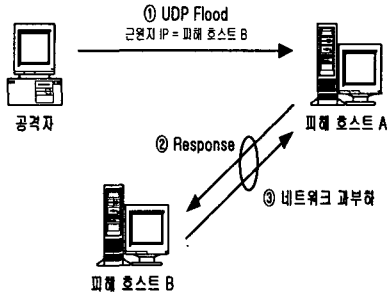
TCP Flooding 공격은 TCP(Transmission Control Protocol)의 연결 지향성의 취약점을 이용한 DoS 공격이다. TCP의 연결 과정인 Three-way handshaking 방식을 이용하여 공격자가 피해 호스트에 근원지 IP주소를 스푸핑하여 SYN(Synchronize) 패킷을 특정 포트로 전송하게 되면 이 포트의 대기큐를 가득 차게 하여 이 포트에 들어오는 연결요청을 큐가 비어 있을 때까지 무시하도록 하는 방법이다.



▶▶ 그림 2. TCP Flooding 공격

2. UDP Flooding 공격

UDP(User Datagram Protocol)를 이용한 패킷 전달은 비연결형 서비스로서 포트 대 포트로 전송한다. 대표적인 응용 서비스로 TFTP, SNMP, 실시간 인터넷 방송이다. UDP Flooding은 UDP의 비연결성 및 비신뢰성 때문에 공격이 용이한 방법이다. UDP는 근원지 IP 주소와 근원지 포트를 스푸핑하기 쉽기 때문에 과다한 트래픽을 피해 호스트에 전송함으로써 시스템 자원과 네트워크를 마비시킨다. UDP Flooding을 나타낸다.

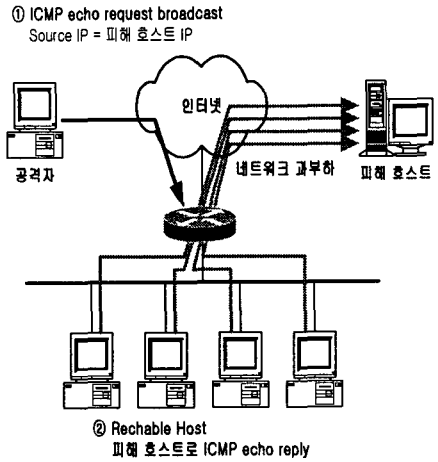


▶▶ 그림 3. UDP Flooding 공격

3. ICMP Flooding 공격

ICMP(Internet Control Message Protocol)은 호

스트간 혹은 호스트와 라우터간의 에러 상태 혹은 상태 변화를 알려주고 요청에 응답을 하는 기능을 담당하는 네트워크 제어 프로토콜로써 활성화된 서비스나 포트가 필요하지 않는 유일한 프로토콜이다. 이를 이용하여 공격자는 대량의 ICMP echo request 메시지를 근원지 IP 주소를 피해 호스트의 IP 주소로 변환하여 보내고 변형된 ICMP echo request 메시지를 받은 호스트들은 피해 호스트로 ICMP echo reply 메시지를 전송하여 피해 호스트에 대량의 트래픽을 발생시키는 ICMP Flooding 공격을 하고 있다.



▶▶ 그림 4. ICMP Flooding 공격

본 논문에서는 위와 같은 공격을 탐지하기 위해서 프로토콜별로 TCPInErrs, UdpNoPorts, Icmp6OutEchoReplies의 MIB(Management Information Base)객체를 이용하여 공격을 탐지한다.

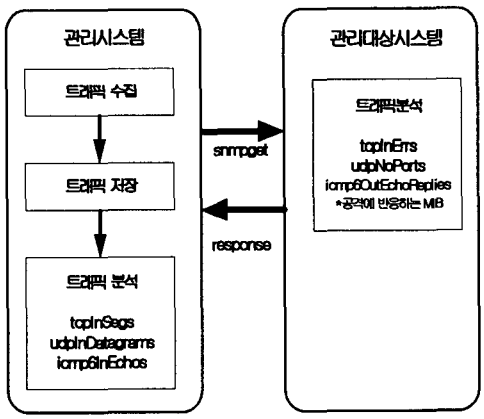
III. IPv6 환경에서 SNMP 이용한 공격 탐지

IPv6 환경에서 SNMP를 설치하고 공격에 민감하게반응하는 TCPInErrs, UdpNoPorts, Icmp6OutEcho Replies의 MIB 객체를 사용하여 유해 트래픽을 검출한다.

[표 1] 공격에 반응하는 MIB 객체

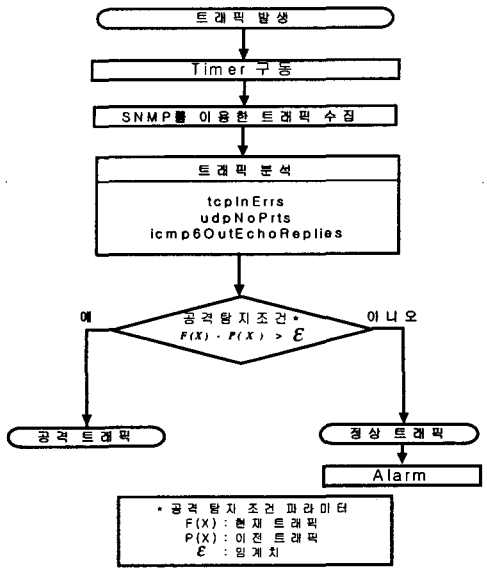
MIB 객체	설명
tcpInErrs	오류로 수신된 세그먼트의 총 개수
udpNoPorts	목적지 포트에 응용 프로그램이 없는 경우 수신된 UDP 데이터그램의 총 개수
Icmp6OutEchoReplies	송신된 ICMP 요청 메시지의 총 개수

관리 시스템에서는 주기적으로 snmpget 명령어를 이용하여 관리 대상 시스템으로부터 트래픽을 수집하게 된다. 단위 시간동안 누적된 입력 트래픽 양을 알기 위해 이전의 누적값에서 현재의 누적값과의 차이를 구한다.



▶▶ 그림 5. 공격 탐지 구조

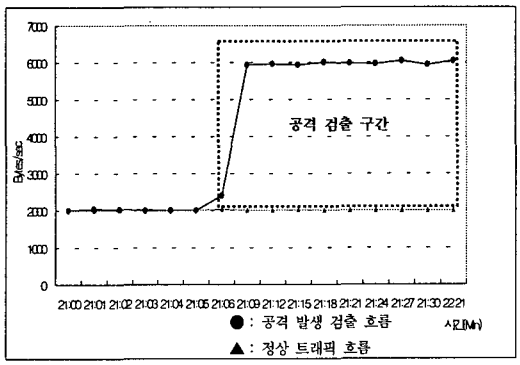
임계치 ε 는 이전 누적값과 현재 누적값의 차이로 공격을 판단하는 기준이 된다. 수집된 트래픽이 공격이 아닐 경우는 일반적으로 침입에 의해 시스템이 다운되기 전까지의 시스템이 정상적으로 유지될 수 있는 5분 동안에 트래픽 분석 유예를 두어 효율적으로 관리되는 시스템을 선택 했으며, 1분 단위의 트래픽 분석시간 동안 공격이 탐지가 되면 관리자에게 Alram 메세지를 보낸다.



▶▶ 그림 6. IPv6 환경의 트래픽 수집 및 분석 알고리즘

VI. 실험 및 결론

본 논문에서 제안한 알고리즘을 실험하기 위해 IPv6를 지원하는 NET-SNMP를 설치하였으며, 공격이 발생하였을 경우, 아래와 같은 공격 검출이 이루어 졌다. 공격과 동일 시간대의 정상 트래픽이 들어올 경우를 비교하기 위해 테스트를 거쳐 정상트래픽의 평균을 아래와 같이 정상트래픽 흐름으로 도시하였다.



▶▶ 그림 7. 트래픽 검출 흐름도

V. 결 론

본 연구에서는NET-SNMP를 이용하여 네트워크에서 관리되는 MIB(Management Information Base) 객체를 통해 누적된 정상 트래픽의 평균 임계치와 실시간 트래픽을 비교하여 신속한 공격 검출이 가능하도록 한다.

향후 MIB 객체의 프로토콜별로 공격을 나누어 자세히 분석할 수도 있으며, 요일의 특성을 살려 트래픽을 검출한다면 관리자에게 보다 다양한 정보를 제공해 줄 수 있을 것이다. 본 논문의 결과는 IPv6 환경에서 불필요한 트래픽을 차단하고 효율적인 망을 운영하기 위한 정보로써 불필요한 경제적 손실을 줄여 사용자의 권익을 보호하는데 활용될 것이다.

IPv6 기반의 본 연구가 네트워크 보안도구인 IDS나 IPS에 활용된다면, 향후 IPv6 환경으로 전환될 때 발생하는 공격 트래픽을 검출할 수 있다.

▌참 고 문 헌▐

[1] 유대성, 구향옥, 오창석, "SNMP를 이용한 유해 트래픽 분석", 한국콘텐츠학회 2004 추계 종합학술대회, pp.215-219, 2004.
[2] 오창석, 생동하는 TCP/IP 인터넷, 내하출판사, 2004.
[3] IPv6 동향 2004, 한국전산원
[4] B. W. Uri Blumenthal. User-based security model (usm) for version 3 of the simple network management protocol. RFC 2574, Apr 1999.
[5] M. Daniele. IP version 6 management information base for the transmission control protocol. RFC2452, Dec 1998.
[6] M. Daniele. IP version 6 management information base for the user datagram protocol. RFC 2454, Dec 1998.
[7] M. J. G H. G. Armitage, P. Schulter. IPv6 over non-broadcast mutiple access (nbma) networks. RFC 2491, Jan 1999.