IPv6 환경에 적용 가능한 트래픽 모니터링 툴

Traffic Monitoring Tool Applicable to IPv6 Environment

이홍규, 김선영, 구향옥, 김영기, 오창석
충북대학교

Lee Hong-Kyu, Kim Sun-Young, Koo Hyang-Ohk,
Kim Young-Gi, Oh Chang-Suk
Chungbuk Univ.

요약

인터넷 사용자의 급격한 증가로 인해 IPv4 주소가 고갈되어 IPv6 기반의 환경으로 전환될 것이다. 본 논문에서는 기존 DDoS 공격을 IPv6 망에서 동작할 수 있도록 수정하고, IPv6 기반의 트래픽 모니터링 툴을 개발한다. 또한, 공격 탐지 알고리즘을 개발 후, 탐지 시스템에 탑재하여, IPv6 상에서 발생할 수 있는 공격 트래픽을 탐지하고 효과적으로 차단할 수 있는 시스템을 구축한다.

Abstract

Recently, Internet user grows larger every year. So, It brought about lack of IP address. Because of it, IPv4 is being substituted to IPv6. In this thesis, proposed attack tool in IPv6 base, attack detection tool have algorithm which is consist of 2 steps attack confrontation with analysis packet header data using packet capture. and automatic attack isolation tool against attack using tool.

I. 서 론

최근에 들어 인터넷 사용자가 늘어나면서 IP 주소의 고갈 현상이 두드러지게 나타나고 있다. 물론 32비트의 IP 주소 공간은 약 40억대의 주소를 할당할 수 있지만 초창기의 인터넷 관리 기관에서는 이 수를 무한에 가깝다고 인식하였으므로 순차적이고 체계적인 주소 할당을 하지 못하였다. 이런 상황들로 인해 각국의 인터넷 관리 기관들은 기존의 IPv4 체계에서 IPv6 체계로의 이향을 서두르고 있는 실정이다.

그러나 이런 급변하는 인터넷 상황에 비해 IPv6로 대체되었을 때의 보안 문제 연구는 상당히 미비한 상태이다. IPv6 체계로 변화하게 되면 헤더 포맷의 변화와 처리 방식의 변화로 인해 설계 당시 생각하지 못했던 버그나 문제점이 발생할 가능성이 많다.

특히, 아직 실제 운용되고 있는 체계가 아니므로, 트래픽에 대한 검증이 이루어지지 못했고, 또한 기존의 IPv4 망에서 이루어졌던 공격들이 IPv6 망에서 어떤 영향을 줄 것인지는 아직 미지수이다.

기존의 트래픽 분석 도구들은 IPv6 트래픽을 탐지할 수 있다 하더라도 단지 공격 탐지만 가능할 뿐이고 오인식률 또한 높아서 시스템의 자원을 낭비하고 있다.

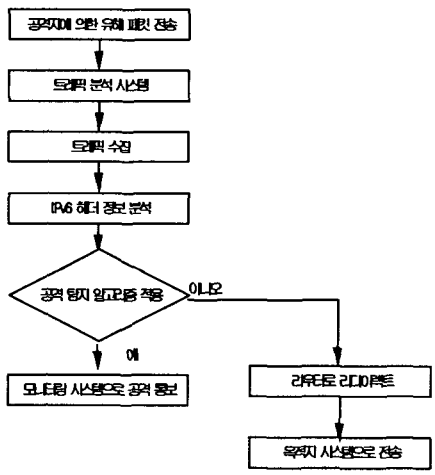
이에 본 논문에서는 차후 IPv6 환경으로 변화되었을 때, 네트워크 환경에 신속하게 대응하기 위하여 IPv6 환경에서 발생할 수 있는 공격 방법을 예측하여 공격을 시도할 수 있는 도구를 구현하고, 그러한 공격을 효율적으로 탐지하여 2단계의 공격 대응을 자동적으로 수행할 수 있는 도구를 구현하였다.

● 본 논문은 충북대학교 유비쿼터스바이오정보기술연구센터의 지원에 의해 수행되었음

2단계로 세분화된 공격 탐지는 오인식률을 크게 줄일 수 있었고, 자동화된 공격 대응 구조는 DDoS 공격에 신속하게 대응하여 시스템 사용률을 감소시킬 수 있음을 보였다.

II. 기존의 IPv6 트래픽 모니터링 도구

대부분의 트래픽 모니터링 도구들은 IPv4 기반의 도구이기 때문에 IPv6 트래픽을 모니터링 할 수 없다. 또한 시험망 기반의 IPv6 탐지 도구라 할지라도 탐지 효율이 낮고, 공격을 탐지하더라도 자동적으로 차단시켜줄 수 있는 기능이 없다. 그림 1은 IPv6 기반 공격 탐지 도구인 IPv6analyzer의 동작 흐름도이다.



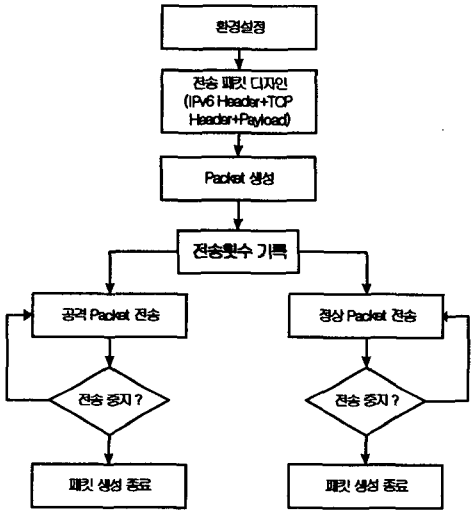
▶▶ 그림 1. IPv6analyzer의 동작 흐름도

IPv6analyzer는 패킷 캡쳐를 이용하여 패킷을 수집해 그 데이터로 공격 여부를 판정하는 구조로 되어 있고, 공격으로 판정하면 모니터링 시스템에 경고 신호를 보낸다.

III. IPv6 기반의 트래픽 모니터링 툴

1. 공격 도구

기존 실험 환경에서는 실제적인 트래픽이 존재하지 않기 때문에 본 논문에서는 IPv6 상에서 발생할 수 있는 공격을 예측하여 공격 도구로 구현하였고, 또한 기존의 DDoS 공격을 IPv6 상에서 동작할 수 있도록 수정하여 구현하였다. 그림 2는 공격 도구의 흐름도이다.

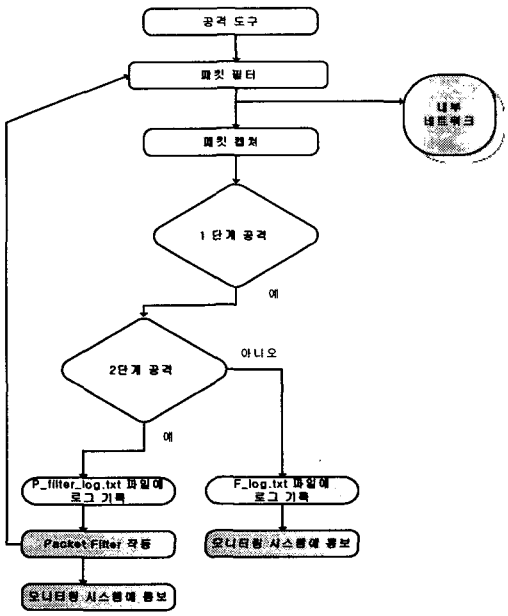


▶▶ 그림 2. 공격 도구의 흐름도

2. 공격 탐지 도구

공격 탐지 도구는 패킷 캡쳐를 수행하여 얻을 수 있는 패킷 헤더 데이터를 통해 트래픽을 분석하는데, 2단계로 세분화 시켜 어떤 대응을 할 것인지를 판단한다. 그림 3은 공격 탐지 알고리즘 흐름도이다.

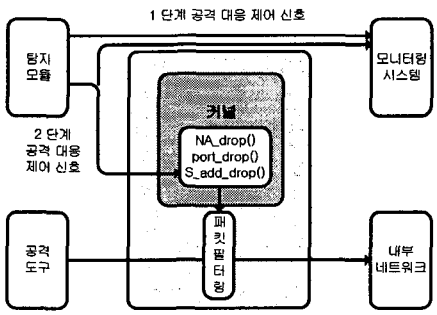
트래픽 탐지 알고리즘은 각 공격별로 2단계의 공격 대응 단계로 판정할 수 있는데 1단계에서는 오탐지의 가능성이 있는 공격을 판단하여 모니터링 시스템에 검토를 요함을 알린다. 2단계는 자동으로 공격 트래픽을 차단해 DDoS 공격에 효율적으로 대처한다.



▶▶ 그림 3. 공격 탐지 알고리즘 흐름도

3. 공격 차단 도구

공격 탐지 도구에서 2단계 공격 대응으로 판정하면 공격 차단 도구에 제어 신호를 보내게 되고 차단 도구는 패킷 필터링을 사용하여 공격 트래픽을 막을 수 있다. 패킷 필터링은 커널 내부에 시스템 콜을 이용하여 구현하였다. 그림 4는 공격 차단 도구의 구조를 나타낸다.



▶▶ 그림 4. 공격 차단 도구의 구조

제어신호에 따라 패킷 필터링을 수행한 후 로그파일에 그 결과를 저장하고 모니터링 시스템에 차단 여부와 그 정보를 알리는 구조로 되어 있다.

IV. 실험 및 결과

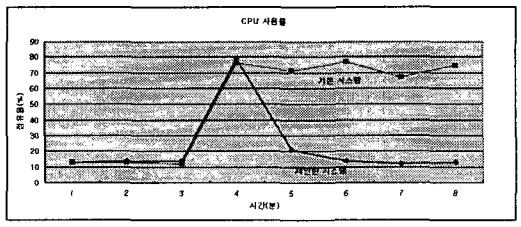
본 논문에서 제안한 도구를 검증하기 위하여 내, 외부에 공격을 위한 에이전트를 설치하여, 제안한 공격 도구를 이용하여 목표 시스템에 공격을 시도하였다.

본 논문에서 제안한 시스템에서 탐지 모듈은 공격 대응 단계를 2단계로 구분해서 감지한다. 공격 에이전트로 4대의 시스템을 사용하였고 이중 1대만 사용한 공격시 탐지되는 공격 정도를 1단계로 정하여 각각의 공격의 임계값을 정해주었다. 그리고 3대의 시스템을 사용하는 경우를 2단계로 정하여 임계값을 구성해 주었다. 표 1은 실험에 의하여 얻어진 임계값들을 나타낸다.

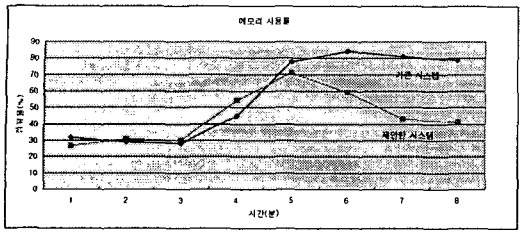
[표 1] 실험에 의한 임계치

공격 방법	DAD-NA	Ext-Hdr	TCP-SYN	UDP-Flood	ICMP-Flood
임계치 A	13	12	13	9	9
임계치 B	30	5	2/3	-	-

제안한 트래픽 도구와 기존 도구인 IPv6analyzer에 각각 DAD-NA 메시지 공격과 UDP flooding 공격을 동시에 보내, 공격 전, 후의 CPU 사용률과 메모리 사용률을 비교하였다. 결과치는 10번의 공격을 시도하여 그 평균값을 사용하였다. 그림 5, 6에서 기존 도구와 제안한 도구의 공격 차단 전, 후의 시스템 사용률을 비교하였다.



▶▶ 그림 5. 공격 차단 전, 후의 CPU 사용률 비교



▶▶ 그림 6. 공격 차단 전, 후의 메모리 사용률 비교

그림 5에서 볼 수 있듯이 공격 발생 후 5분간의 CPU 사용률은 제안한 시스템이 47.4%의 개선 효과를 보이고 그림 6에서는 제안한 시스템의 메모리 사용률이 19.8% 개선됨을 볼 수 있다.

기존 IPv6analyzer와 2단계 공격 대응을 사용하는 제안한 시스템의 오인식률을 비교하기 위하여 4대의 시스템으로 공격 프로세스의 수를 증가시키면서 공격을 가하고, 그 때 처음 공격을 인식하는 순간의 공격 프로세스 수를 구하였다. 결과치는 10번의 실험 평균으로 구하였다. 표 2에 공격 도구 종류별로 공격 탐지시의 공격 프로세스 수를 나타내었다.

[표 2] 공격 탐지시의 공격 프로세스 수

	DAD-NA 메시지 공격	Ext-Hdr 공격	TCP-SYN Flooding	UDP Flooding	ICMP Flooding
기존 시스템	17	32	34	14	19
제안 시스템	8	23	9	5	11

즉, 제안한 시스템은 평균 47.8% 정도 오인식률이 개선됨을 알 수 있다.

표 3에 기존 도구와 제안한 시스템을 비교하였다.

[표 3] 기존 도구들과 제안한 시스템의 기능 비교

도구 / 비교대상	Ethereal	IPv6analizer	제안 시스템
분석 대상	IPv6 패킷	IPv6 패킷	IPv6 패킷
공격 탐지	수동 ,부정확	가능	2단계 가능
공격 차단	수동 차단	수동 차단	자동 차단
공격 대응 시간	공격 탐지 시간 수동 공격 차단 시간 수동	공격 탐지 시간 최대 1분 공격 차단 시간 수동	공격 탐지 시간 최대 1분 공격 차단 시간 자동(탐지시 즉시)

V. 결 론

기존 도구인 Ethereal은 공격 탐지와 공격 차단 모두 수동으로 처리하기 때문에 빠른 대응을 하기 어렵고, IPv6analyzer도 탐지는 자동으로 수행하지만 공격 대응 부분이 수동으로 처리되기 때문에 신속한 대응이 요구되는 DDoS 공격에 대응하기 어렵다. 본 논문에서 제안한 IPv6 기반 자동화된 공격 탐지 및 차단 도구는 2단계 공격 대응 단계를 사용함으로써 오인식률을 크게 감소시킬 수 있고, 공격 탐지 알고리즘에 의해 공격이 탐지되었을 때 자동화된 대응을 통하여, DDoS 공격에 필수적인 빠른 대응을 가능하게 함을 실험을 통해 보였다.

향후 과제로는 MIB를 이용한 공격 탐지를 결합하여, 패킷 헤더를 이용한 탐지시 발생할 수 있는 오인식률을 최소화하는 것이 필요하고, 탐지 시스템을 분산시켜 더 효율적이고 안정적인 탐지 및 대응 시스템을 구축하는 것이 필요하다.

▮참 고 문 헌▮

[1] 오창석, 생동하는 TCP/IP 인터넷, 내하출판사, 2004.
[2] 김용진외 3명, 차세대 인터넷 프로토콜 IPv6, 다성출판사, 2003.
[3] T. Nordmark, E. Simpson, "neighbor Discovery for IP Version 6" RFC 2461, 1998.
[4] W. Stevens, TCP/IP Illustrated Volume 1,2, Addison-Wesley, 1994.
[5] 권상호외 3명, Unix & Linux C Programming, 영진출판사, 2002.
[6] D. Moore, G. M. Voelker, S. Savage, "Inferring Internet Denial of Service Activity," Univ. of California, 2001.
[7] 김선영, 이홍규, 오승희, 서동일, 오창석, "IPv6 기반 트래픽 분석 도구 설계", 한국콘텐츠학회 논문지, 제 5 권 2호, (pp.115-121), 2005.