韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-2-8

IPv6 기반 자동화된 공격 대응도구

이 홍 규*, 구 향 옥**, 김 선 영***, 김 영 기****, 오 창 석 *****

Automatic Attack Reaction Tool Based on IPv6

Hong-Kyu Lee*, Hyang-Ohk Koo**, Sun-Young Kim***, Young-Gi Kim****, Chang-Suk Oh*****

요 약

본 논문에서는 IPv6 기반 자동화된 공격 대응도구 알고리즘을 제안하였다. 현재는 IPv6에서 사용할 응용 프로그램 및 표준화에 초점을 두고 연구가 진행중에 있어 향후 IPv6의 보안에 대해서는 아직 연구가 미흡한 상태이다. 본 논문에서 제안한 방법은 IPv6에서 발생할 수 있는 공격과 기존 IPv4에서의 공격을 탐지하고 자동화된 대응방법을 통해 개인의 정보보호가 가능하다. 일반적으로 침입 탐지 시스템의 경우 탐지만 하기 때문에 피해는 계속 반복적이다. 따라서 본 연구에서는 이러한 문제점을 직시하고 조기에 연구함으로써 문제 해결방안을 제시하고자 한다. 본 논문에서 제안한 알고리즘은 리눅스 기반에서 IPv6망을 구축하여 실험 하였다. 실험 결과, 제안한 알고리즘을 이용하여 효율적으로 공격을 검출할 수 있었다.

Abstract

In this paper proposed automated attack reaction tool based on IPv6. Currently, much researches are performing focused on application program and standardization for IPv6. But, It is not enough for future IPv6 security. The proposed method detect attacks on IPv6 and conventional IPv4, therefore it is possible to protect personal information using automated reaction method. Usually, IDS just perform detection, therefore damages may be repeated. However, this paper considered the problems described above, and suggested solution for this problems. The proposed algorithm suggested in this paper is simulated on IPv6 network based on Linux. As a simulation result, it is proved that proposed algorithm can detect attacks efficiently.

▸ Keyword : IPv6, Intrusion Detection, Automatic Attack Reaction, Web based Monitoring

---

• 제1저자 : 이홍규
• 접수일 : 2005.06.07, 심사완료일 : 2005.07.10
*, **, ***, **** 충북대학교 컴퓨터공학과, ***** 충북대학교 전기전자컴퓨터공학부
※ 이 논문은 충북대학교 유비쿼터스바이오정보기술연구센터의 지원에 의해 수행되었음.

Ⅰ. 서 론

1.1 연구의 필요성

첨단 정보통신기술의 발달에 따라 정보와 지식의 창출, 정보의 유통 및 활용이 자유로워짐으로써 여러 부문에서 국가경쟁력이 제고되고 국가이익의 극대화 및 국민편익의 향상을 도모할 수 있게 되었다. 그러나 최근 들어 이러한 정보화의 순기능 못지않게 전산시스템에 대한 해킹, 컴퓨터 바이러스의 유포, 음란물의 유통, 개인정보의 오·남용, 지적재산권의 침해 등 많은 역기능 현상들이 나타나고 있다. 뿐만 아니라 이러한 역기능 현상의 종류가 다양해지고 지능화되면서 양적인 면에서도 증가 일로에 있어, 피해의 양상이 점점 더 심각한 상태로 치닫고 있는 실정이다. 이러한 피해는 비단 IPv4에서만 발생하는 것은 아니다. 향후 현재의 IP 부족문제를 해결하기위해 IPv6환경[1][2]으로 변화할 경우에 그 피해는 지금과는 비교할 수 없을 정도로 상당하다. 그러나 이러한 큰 피해[3]가 예상됨에도 불구하고 현재는 대부분이 IPv6에서 사용가능한 응용프로그램 및 표준화에 초점을 맞추어 연구중에 있고 IPv6에서 보안 문제는 아직 미흡한 실정이다. 따라서 본 논문에서는 향후 IPv6한경에서 그 피해 규모와 개인의 정보 보호를 위해 IPv6 기반 자동화된 대응도구에 관한 연구를 조기에 수행하여 향후 국내 보안 산업 및 학계에 보안 연구의 발판을 제공하게 될 것이다.

1.2 연구 목적

본 연구는 향후 IPv6 환경이 도래할시 발생하는 수많은 유해 트래픽으로부터 개인의 정보 보호와 시스템 자원을 보호함에 연구의 목적을 두고, 연구의 광범위한 특성상 IPv4 기반침입탐지 및 침입 차단에 대한 기초 연구 및 방법에 대한 분석 등의 이전 연구를 바탕으로 IPv6에서 자동화된 대응도구에 관한 연구를 실시하였다. 본 연구에서는 IPv6에서 유해 트래픽 탐지 알고리즘 설계 및 개발과 자동화된 대응도구를 통해 보다 효율적이고 안전한 통신을 보장하는 것이다.

Ⅱ. 기존 탐지 방법

IPv6 기반 공격을 탐지하는 방법은 서론에서 언급하였듯이 현재는 IPv6 환경에서 사용할 수 있는 응용프로그램 및 표준화에 대해서만 연구가 진행되고 있기 때문에 IPv6에서 탐지 방법은 연구된 것이없다. 따라서 본 연구를 위해서는 IPv4에서 탐지하는 방법을 이해 및 분석을 통해 IPv6에서 발생 가능한 공격과 기존에 IPv4에서의 사용되었던 공격들이 재사용 할 수 있는 방법에 대하여 연구하였다. 본 절에서는 지금까지 제안된 IPv4에서 탐지 및 대응에 관한 기법에 대하여 살펴본다.

2.1 침입 탐지의 분류 및 방법

2.1.1 침입행위의 결과에 따른 분류.

일반적으로 침입이란 비인가된 사용자가 자원의 무결성, 기밀성, 가용성을 저해하는 일련의 행동들과 보안 정책을 위반하는 행위를 말한다. 따라서 침입 탐지는 이러한 위반된 행위를 탐지하는 것을 말한다. 침입 탐지는 침입 행위의 결과에 따른 분류, 침입 자료의 근거에 둔 분류로 나뉜다. 침입 행위의 결과[4][5][6]에 따른 분류는 다시 데이터 소스 기반, 침입 탐지 모델 기반으로 분류할 수 있다. 〈표 1〉은 침입 탐지의 분류를 나타내었다.

표 1. 침입 탐지 분류
Table 1. Classification of intrusion detection

데이터 소스 기반	단일 호스트 기반 침입 탐지
	다중 호스트 기반 침입 탐지
	네트워크 기반 침입 탐지
침입 탐지 모델 기반	비정상 침입 탐지
	오용 침입 탐지

침입 탐지는 데이터 소스를 기반으로 호스트 기반, 다중 호스트 기반, 네트워크 기반으로 분류된다. 또한 침입 탐지 모델을 기반으로 한 분류 방법에서는 비정상 침입 탐지와 오용 침입 탐지 기법이 있다. 비정상 침입 탐지 기법은 공

격자가 공격 시 침입 탐지측에서는 사용자의 패턴을 분석하여 입력 패턴과 비교하는 탐지 방법이다. 따라서 정형화된 모델을 선정한 후 벗어나는 경우만 침입으로 탐지하는 방법을 말한다. 비정상 침입 탐지 기법의 종류로는 예측 가능한 패턴 생성, 통계적 방법, 신경망 등이 있다. 다음으로 오용 침입 탐지 기법은 알려진 침입 행위를 이용하여 침입을 탐지하고 정해진 모델과 일치하는 경우를 침입으로 간주하는 기법이다.

2.1.2 침입 자료의 기반에 따른 분류

- **호스트 기반 침입 탐지**
  Program, Process의 변수, OS에서 기본적으로 제공하는 Log기록을 통해서 감사자료를 수집, 침입탐지에 이용하는 방법이다.
- **네트워크 기반 침입 탐지**
  Network 상에 흐르고 있는 packet을 수집하여 protocol을 해석, 감사자료로 사용하는 방법이다.
- **다중호스트 기반 침입 탐지**
  다중호스트에서 순차적인 아닌 다중적으로 단일 host에 침입하는 형태의 침입을 탐지하는 방법이다

(그림 1)은 일반적으로 가장 많이 사용되고 있는 네트워크 기반 침입 탐지 방법을 도시하였다.

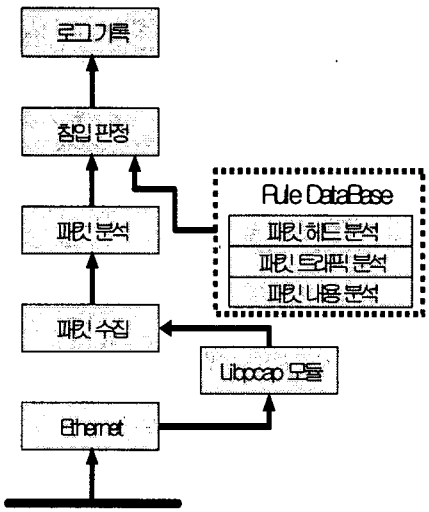


그림 1. 네트워크 기반 침입 탐지
Fig. 1. Network based intrusion detection

2.2 침입 방지 기술

침입 방지와 침입 탐지의 근본적인 차이점은 침입 탐지는 침입이 발생했을 때 문제를 즉각적으로 처리하지는 못하지만 침입 방지[7]는 공격 시그너처를 찾아내고 네트워크의 트래픽을 관찰해, 수상한 활동을 하는 패킷에 조치를 취한다는 것이다. 또한, 침입 방지 기술은 서버가 비정상적인 행동을 할 경우 자동으로 실행을 중단할 수 있다는 것이다. 이러한 침입 방지 기술은 침입 탐지 기술과 마찬가지로 호스트 기반과 네트워크 기반으로 분류할 수 있다. 호스트 기반 침입 방지 기술의 특징은 크게 커널과 함께 동작해 커널 이벤트를 가로채 처리하는 방식과 커널과 독립적으로 작동하는 방식으로 구분되면, 전자는 대부분 접근 제어 기능을 가진 신뢰할 수 있는 운영체제 제품들로 분류할 수 있다. 그러나 후자는 시그너처와 행동 기반 분석 알고리즘을 이용 특정 규칙에 위배되는 이벤트를 필터링하는 기술이다. 침입 대응의 방법은 다음과 같다.

- **통지**
  침입 탐지 사실을 콘솔에 표시하거나 관리자에게 SMS, E-mail 등으로 통지
- **세션 차단**
  보다 적극적인 방법으로 침입이 이루어지고 있는 해당 연결 세션을 차단시킨다.
- **라우터 및 침입 방지 기술과 연동**
  세션 차단 보다 더 적극적인 방법으로 라우터나 침입 차단 기술과 연동하여 접근을 봉쇄하는 기술이다.

III. IPv6 기반 자동화된 공격 대응도구

3.1 전체 시스템 구성

본 시스템은 IPv6에서 발생 가능한 공격을 탐지하고 자동화된 공격 대응을 통해 네트워크와 시스템의 과부하를 방지하는 것을 목적으로 기존의 IPv4에서 공격을 탐지하고 대응하는 현재의 일반 시스템들과 구별되는 특징을 가진다. IPv6 기반 자동화된 공격 대응을 위해서는 공격자가 IPv6에서 공격을 할 수 있도록 공격 도구 설계와 함께 IPv6 망 구성이 조성되어야 한다. 이런 IPv6 망을 구축한 후 자동화

된 공격 대응 도구를 설계 하였다. 자동화된 공격 대응도구의 환경은 공격 모듈, 탐지 모듈, 차단 모듈, WEB 기반 모니터링 모듈로 구성된다. 공격 모듈에서는 IPv6에서 발생 가능한 공격 및 IPv4에서의 공격 재조립을 수행하여 공격하게 된다. 공격 대응 시스템에서는 리눅스 기반에서 실시간으로 네트워크에서 IPv6 트래픽을 수집하게 된다. 수집된 트래픽은 버퍼를 통해 탐지 모듈에의 공격 여부를 판단하게 된다. 탐지 모듈에 의해 공격으로 판정된 트래픽에 대해서는 차단 모듈을 통해 차후 재공격이 불가능하도록 IP와 포트등을 차단하게 되고 또한 공격으로 탐지된 결과에 대해서는 관리자가 다른 실시간으로 WEB에서 모니터링이 가능하다. (그림 2)는 IPv6 기반 자동화된 공격 대응도구의 구성도를 도시하였다.

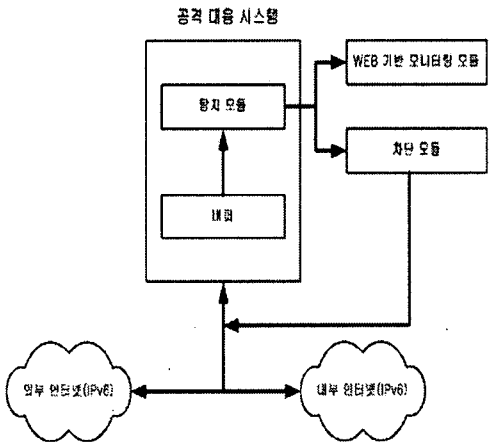


그림 2. 자동화된 공격 대응 시스템 구성도
Fig. 2. Architecture of automatic attack reaction system

3.2 공격 모듈

본 논문에서 구현한 공격 도구는 IPv6에서 발생 가능한 공격과 IPv4에서 인터넷 계층만의 수정으로 사용가능한 공격을 설계 하였다. 공격의 종류로는 IPv6에서 발생할 수 있는 DAD-NA(Duplicate Address Detection Neighbor Advertisement) 공격, 확장헤더를 이용한 공격, 플로우 레이블을 이용한 공격 및 IPv4 공격을 재조립한 TCP, UDP, ICMP 플러딩 공격을 실험 대상으로 하였다. 공격 모듈은 Netwib 라이브러리를 이용하여 원하는 유해 트래픽을 생성하여 자동 공격할 수 있도록 설계 하였다.

• DAD-NA 공격의 특징

DAD-NA 공격은 IPv6 환경에서 새로이 도입된 비상태형 주소 자동 설정 방법의 취약점을 이용하여 라우터의 성능을 저하시키는 공격이다. DAD-NA[8][9] 공격은 ICMP를 type 136 request를 이용하여 메시지를 요청하는 공격이다. 공격은 (그림 3)과 같다. 라우팅 테이블에 있는 주소를 이용하여 목적지 주소와 근원지 주소를 동일하게 넣고 NA 메시지를 전송하게 된다. 이렇게 됨으로써 해당 주소를 가지고 있는 호스트는 같은 주소에 의해 NA를 받게 되므로 주소 충돌이라고 인식하게 된다. 주소 충돌을 감지한 호스트는 해당 주소를 자동으로 재설정하게 되는데 이때 라우터와 RA, RS 메시지를 이용하여 새로운 주소를 설정하게 된다. 만약 라우터 내부에 있는 호스트의 주소가 많으면 많을수록 동시 다발적으로 발생하는 RS, RA 메시지의 양은 많아지게 되므로 서비스 거부 공격이 가능하다.

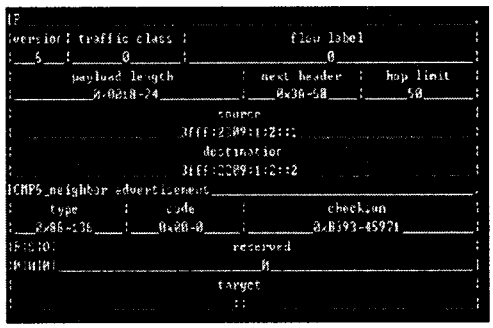


그림 3. DAD-NA 공격의 헤더
Fig. 3. Header of DAD-NA attack

• TCP 플러딩 공격

TCP 플러딩 공격은 IPv4와 유사하게 TCP 연결설정 과정중 클라이언트에서 서버로 연결요청을 한후 서버에서 TCP SYN[10] 플래그 설정하게 되면 연결요청에 대한 ACK 를 받고 ACK 신호에 대한 확인 메시지를 보내지 않으므로 발생하는 서비스 거부 공격이다. (그림 4) TCP 플러딩 공격을 설정한 그림이다.

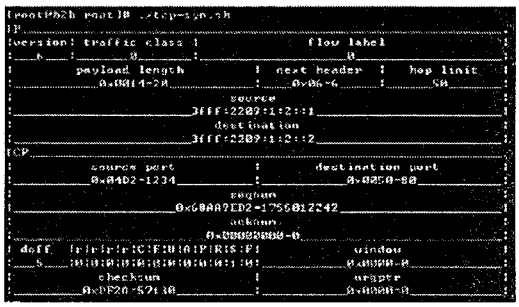


그림 4. TCP 플러딩 공격의 헤더
Fig. 4. Header of TCP flooding attack

• UDP 플러딩 공격

UDP 플러딩 공격은 피해 호스트를 설정하여 대량의 UDP[11] 패킷을 전송하는 트래픽 폭주 공격이다. UDP 플러딩 공격의 특징이 31337, 31335와 같은 특정 포트로 설정하여 트래픽을 전송하는 공격이다. 공격은 수신측에 계속적인 UDP플러딩 패킷을 보냄으로써 정상적인 서비스를 할 수 없게 만드는 과정이다. (그림 5)는 UDP 플러딩 공격을 위해 패킷을 조립한 그림이다.

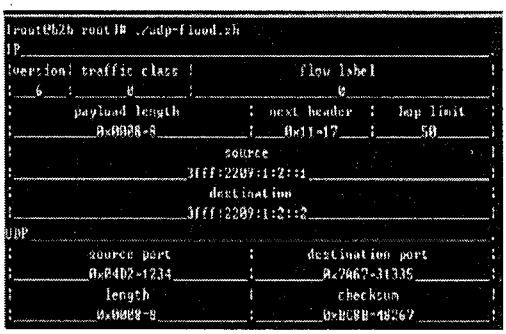


그림 5. UDP 플러딩 공격의 헤더
Fig. 5. Header of UDP flooding attack

• ICMP 플러딩 공격

ICMP 플러딩 공격은 ICMP echo request를 이용하게 된다. 일반적인 응용프로그램 ping과 유사하게 icmp echo request를 받은 시스템은 항상 icmp echo reply를 해줘야한다. 요즘은 운영체제에서 차단하는 경우도 있지만 대부분의 사용자들이 편의를 위해 ping포트를 오픈해놓기 때문에 이러한 공격이 가능하다. 따라서 공격자는 imcp echo request에 해당하는 type을 128로 설정하여 초당 수 천개의 패킷을 피해 호스트로 전송하게 되면 피해 호스트는 대량의 유해트래픽으로 인해 정상적인 서비스를 제공할 수 없게 하는 공격이다. (그림 6)은 ICMP 플러딩 공격 헤더를 설계한 그림이다.

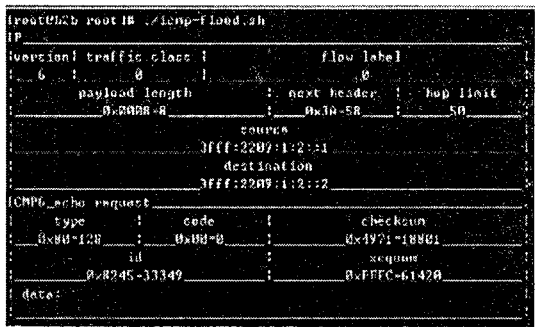


그림 6. ICMP 플러딩 공격의 헤더
Fig. 6. Header of ICMP flooding attack

3.3 탐지 모듈

탐지 모듈은 공격 모듈에서 공격을 수행하였을 경우 네트워크에서 트래픽을 수집한 결과를 이용하여 공격 여부를 탐지하는 알고리즘이다. 탐지 모듈의 전체 흐름도는 (그림 7)과 같다. 탐지 모듈은 네트워크 기반이므로 네트워크상의 모든 트래픽을 수집하게 된다. 수집된 트래픽들은 헤더 정보에서 분석을 위해 수집 시간, 프로토콜, 출발지 주소 목적지 주소를 추출하여 탐지 알고리즘에 의해 공격 여부를 판단하게 된다.

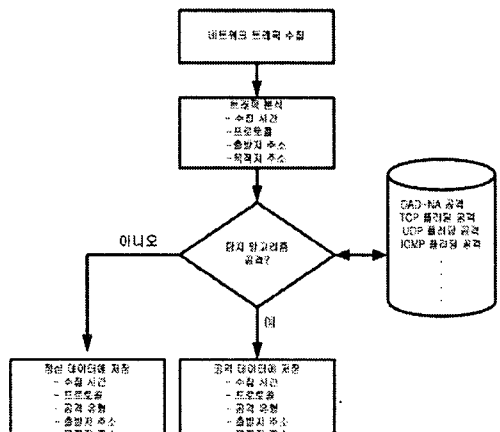


그림 7. 탐지 모듈의 흐름도
Fig. 7. Flow of detection module

탐지 모듈 알고리즘은 (그림 8)과 같다. 먼저 Pacpetcapture 함수[12]를 이용하여 네트워크 기반의 패킷을 수집한 후 ipv6save 구조체에 필요한 정보를 저장하게 된다. 다음으로는 Detectmodule함수를 이용하여 공격 데이터베이스에 있는 공격 종류와 일치하게 되면 해당 차단 모듈을 호출하고 로그파일을 남기게 된다. 정상일 경우는 서비스를 내부 네트워크로 송수신이 허용되게 된다.

```
Packetcapture(); // (save to ipv6save( ))
Detectmodule();
{
   if(ipv6save( ) is DAD_NA)
      {
      Preventionmodule(na);
      Save to logfile (na.txt)
      }
   if(ipv6save( ) is EXT)
      {
      Preventionmodule(ext);
      Save to logfile (ext.txt)
      }
   if(ipv6save( ) is TCP_SYN)
      {
      Preventionmodule(tcpsyn);
      Save to logfile (tcp-syn.txt)
      }
   if(ipv6save( ) is UDP_flood)
      {
      Preventiondodule(udpflood);
      Save to logfile (udp-flood.txt)
      }
   if(ipv6save( ) is Ping);
      {
      Preventionmodule(ping0;
      Save to logfile (icmp-flood.txt)
      }
} end of DetectModule
Return to Packetcapture();
```

그림 8. 탐지 모듈 알고리즘
Fig. 8. Detection moudule algorithm

3.4 차단 모듈

차단 모듈은 필터링 프로그램인 ip6tables를 이용하여 스크립트 프로그램으로 작성되었다. 탐지모듈에서 공격이 탐지되면 fork()함수로 프로세스를 생성하고 탐지모듈에서 탐지된 공격의 유형과 공격의 유형에 따른 IP정보나 포트번호를 전송하게 된다. 또한 자식프로세스는 전송받은 정보를 인수로 사용하여 필터링 프로그램을 실행한다. 필터링 프로그램은 스크립트로 작성되었고 ip6tables 프로그램의 복잡한 인수를 캡슐화 시켜 공격 차단 알고리즘에 필요한 정보만을 인수로 취할 수 있도록 스크립트 프로그램으로 작성하였다. 부모프로세스는 다음번 공격 탐지를 위해 다시 탐지 모듈을 구동시킨다. (그림 9)는 차단 모듈 흐름도를 도시하였다.

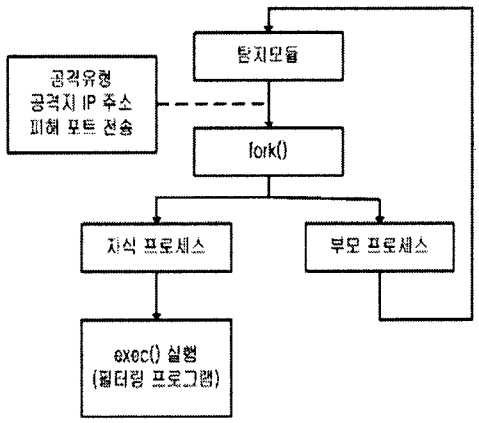


그림 9. 차단 모듈 흐름도
Fig. 9. Flow of Blocking module

3.5 WEB 기반 모니터링 모듈

WEB 기반 모니터링 모듈은 탐지 모듈에 의해 탐지된 공격 트래픽을 이용하여 공격 유형, 공격 시간, 공격별 누적치를 실시간으로 WEB에서 모니터링 할 수 있도록 설계된 모듈이다. WEB 기반 모니터링 모듈을 이용하여 관리자는 장소에 제약 없이 공격 관련 정보를 모니터링하는 것이 가능하다.

Ⅳ. 실험결과

실험환경으로는 리눅스 커널 버전 2.4, 메모리 512 메가 바이트, C, PHP, 펜티엄 4 CPU를 사용하였다. 본 연구의 알고리즘을 구현하여 공격 탐지 가능 여부와 탐지될 결과를 WEB 기반 모니터링 모듈에 나타난 결과 및 차단 모듈에 의해 차단 유무에 따른 CPU 사용율에 대하여 비교하였다.

본 논문에서 제안한 IPv6 기반 트래픽 분석 도구의 성능을 평가하기 위한 실험망은 그림과 같다. 각 호스트는 정상 패킷과 공격 패킷을 생성하여 목표 시스템으로 전송하며, 라우터에서는 IPv6 기반 자동화된 대응도구가 실행되어 내•

외부에서 들어오는 트래픽을 분석하게 된다. DAD-NA 메시지 공격, TCP 플러딩 공격, UDP 플러딩 공격, ICMP 플러딩 공격을 수행한 다음 공격 탐지 유무를 실험하였다. (그림 10)은 실험을 위한 IPv6 실험망에 대한 구성도 이다. IPv6 기반 자동화된 대응도구는 내•외부를 연결할 수 있는 라우터에 데몬으로 실행되고 있다.

실험망을 구축한 후 정상 트래픽과 유해 트래픽에 해당하는 DAD-NA 공격, TCP 플러딩, UDP 플러딩, ICMP 플러딩 공격을 수행하였을 경우 검출 화면은 (그림 11)과 같다. 공격 검출 시 공격 시간, 공격 유형, 공격별 누적치, 공격 횟수를 실시간으로 확인할 수 있었다.

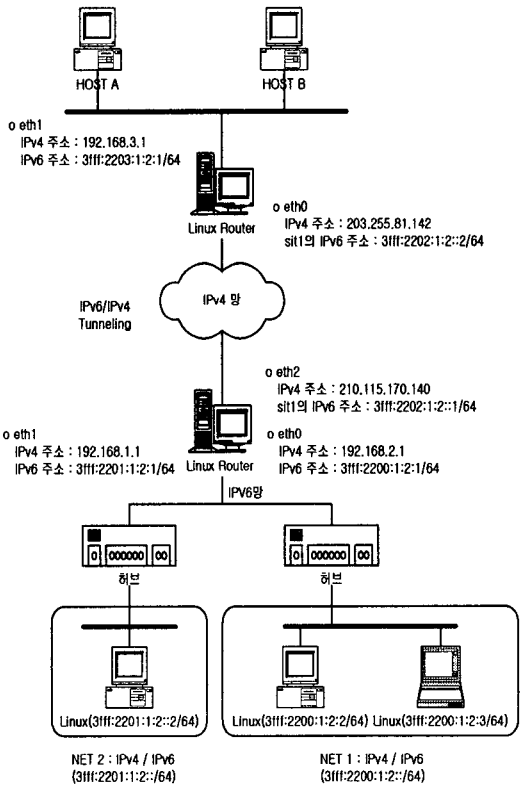


그림 10. 실험망 구성도
Fig. 10. Configuration of test network

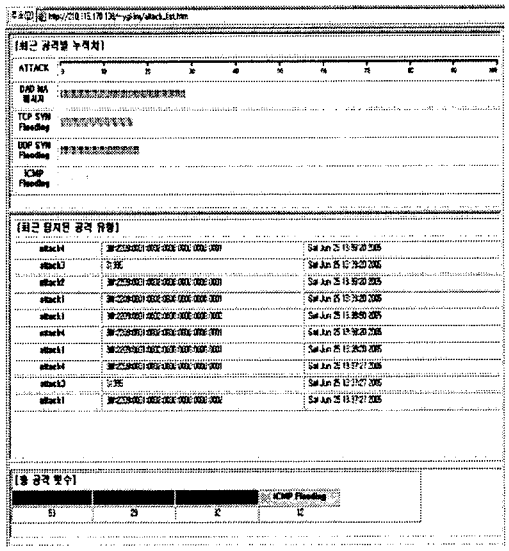
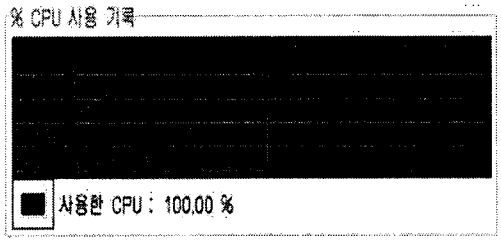
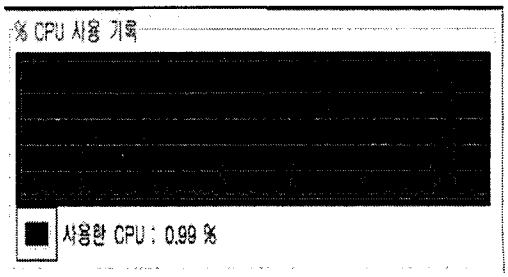


그림 11. 웹 기반의 공격 검출 결과
Fig. 11. Web based attack detection result

(그림 12(a))는 DAD-NA 공격, UDP 플러딩 공격을 수행하여 총 10대의 에이전트에서 각 에이전트당 20개의 프로세스를 실행시켜 초당 10만개의 패킷을 전송하였을 경우 차단 모듈이 구동 되지 않았을 경우 트래픽에 의한 CPU 사용율을 보여준다.



(a) 차단 모듈을 사용하지 않은 경우



(b) 차단 모듈을 사용한 경우

그림 12. CPU 사용량
Fig. 12. CPU usage

(그림 12(b))는 트래픽 폭주 공격을 수행한 후 차단 모듈에 의해 유해 트래픽을 차단 시킨후의 CPU 사용량을 도시하였다.

(그림 13)은 정상적인 기본 서비스만을 제공하는 서버에서의 메모리 사용량과 대응도구가 비활성화 되었을 경우 메모리 사용량, 대응도구가 활성화 되었을 경우의 메모리 사용량을 도시하였다. 실험결과 대응도구를 사용하지 않았을 경우에는 메모리가 유해 트래픽으로 인해 오버플로우가 발생하여 정상적인 서비스를 할 수 없게 되었다. 그러나 대응도구가 활성화 되었을 경우에는 처음 유해 트래픽을 받았을 경우에만 메모리 사용량이 증가했다가 차단되면서 정상 메모리와 비슷함을 확인할 수 있었다.

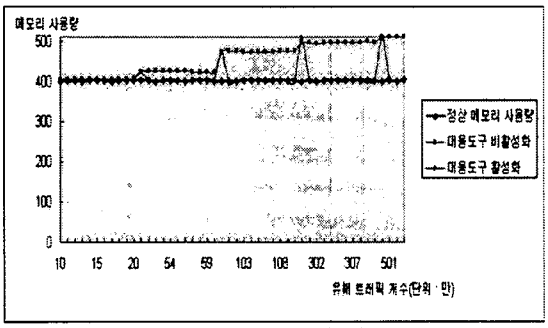


그림 13. 메모리 사용량
Fig. 13. Memory usage

V. 결론

본 논문에서는 IPv6 기반 자동화된 대응도구를 설계하였다. 제안한 자동화된 대응도구를 이용하여 IPv4 기반 수정된 공격 및 IPv6에서 예상 가능한 공격을 탐지 및 대응이 가능함을 확인 할 수 있었다. 그리고 실험을 통해 IPv6 환경이 되어도 기존에 IPv4에서 존재하였던 공격이 인터넷 계층만이 변경되고 상위 계층은 그대로 사용됨으로 기존 공격이 유효하다는 것을 입증되었다. 실험을 통해 알 수 있듯이 제안한 자동화된 대응도구 알고리즘을 통해 신속한 탐지와 탐지 후 자동화된 대응으로 CPU 사용량과 메모리 사용량이 현저하게 줄어드는 것을 확인 할 수 있었다. 향후, 보다 많은 공격 탐지 알고리즘을 추가한다면 IPv6 환경에서 안전하고, 효율적으로 시스템 및 정보보호가 가능하리라 사료된다.

참고문헌

[1] 오창석, 생동하는 TCP/IP 인터넷, 내하출판사, 2004.
[2] 김용진 외2, 차세대 인터넷 프로토콜 IPv6, 다성출판사, 2002.
[3] 조완수, 정보시스템 보안, 홍릉과학출판사, 2003.
[4] 임채호, "최근 해킹기법 분석과 대응책", 제 4회 정보보호심포지움, 한국정보보호센터, 1991. 4.
[5] 이경하 외 3명, "네트워크 패킷 정보를 기반으로 한 보안 관리", 한국정보과학회 논문지 Vol.25, pp.1405-1412, 1998.
[6] T. F. Lunt, "A Survey of Intrusion Detection Techniques," Computer & Security, Vol.12, No.4, 1993.
[7] 조대철, 송규철, 노병구 역, 네트워크 침입탐지와 해킹분석 핸드북, 인포북, 2001.
[8] Paul E. Proctor, Intrusion Detection Handbook, Prentice Hall, 2001.
[9] W. Stevens, TCP/IP Illustrated, Addison-Wesley, 1994.
[10] RFC 2461, Neighbor Discovery for IPv6, 1998.
[11] RFC 2993, Transition Mechanism for IPv6 Hosts and Routers, 2003.
[12] RFC 3056, Connection of IPv6 Domains via Clouds, 2001.
[13] W. Stevens, Unix Network Programming, Prentice Hall, 1999.

저 자 소 개

이 홍 규

2003년 2월 : 충북대학교 컴퓨터공학과(공학사)
2003년 8월~현재 : 충북대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 컴퓨터네트워크

구 향 옥

1999년 8월 한밭대학교 전자계산학과(이학사)
2002년 2월 충북대학교 컴퓨터공학과(공학석사)
2002년~현재 충북대학교 컴퓨터공학과 박사과정
2003년 8월~현재 백석대학 겸임
〈관심분야〉 컴퓨터네트워크, 뉴로컴퓨터, 정보보호

김 선 영

2001년 2월 : 한밭대학교 전자공학과(공학사)
2003년 2월 : 충북대학교 컴퓨터공학과(공학석사)
2003~현재 : 충북대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 컴퓨터네트워크

김 영 기

2005년 2월 : 우송대학교 컴퓨터과학과(이학사)
2005년 3월~현재 : 충북대학교 컴퓨터공학과 석사과정
〈관심분야〉 컴퓨터네트워크, 뉴로컴퓨터, 정보보호

오 창 석

1978년 2월 : 연세대학교 전자공학과(공학사)
1980년 2월 : 연세대학교 전자공학과(공학석사)
1988년 8월 : 연세대학교 전자공학과(공학박사)
1985년~현재 : 충북대학교 전기전자컴퓨터공학부 교수
1982년~1984년 : 한국전자통신연구원 연구원
1990년~1991년 :Stanford대학교 객원교수
2001년~2004년 8월: 한국콘텐츠학회 논문지편집위원장
2004년 9월~현재 : 한국 콘텐츠학회 상임고문
〈관심분야〉 컴퓨터네트워크, 뉴로컴퓨터, 정보보호