네트워크 공격을 탐지하기 위한 IPv6 트래픽 분석 도구

오승희* · 오진태*

*한국전자통신연구원 정보보호연구단 보안게이트웨이연구팀

The Design of IPv6 Traffic Analysis Tool for Detecting Network Attacks

Seung-hee Oh* · Jintae Oh*

*ETRI Information Security Research Division, Security Gateway Research Team

E-mail : seunghee5@etri.re.kr

요 약

인터넷상의 주소 고갈 문제를 해결하기 위해 기존의 IPv4 네트워크를 IPv6 네트워크로 도입하려는 계획이 국내외에서 단계적으로 추진되고 있다. IPv6 네트워크 도입으로 인해 IP 주소 부족 문제는 해결될 수 있으나 기존에 존재하던 네트워크 보안상의 문제점과는 또 다른 형태의 네트워크 공격이 야기될 수 있다는 위험성이 잠재되어 있다. 따라서, 본 논문에서는 IPv6 네트워크 환경에서 발생될 수 있는 네트워크 공격을 차단하기 위한 선행 과정인 IPv6 기반의 트래픽을 효율적으로 분석하는 도구를 제안한다. 구현된 IPv6 트래픽 분석 도구는 IPv6 헤더를 이용하여 트래픽 분석 및 공격을 검출하는 방식으로 공격 검출은 추정 가능한 공격에 대해 제안한 탐지 알고리즘을 이용하고 있다.

ABSTRACT

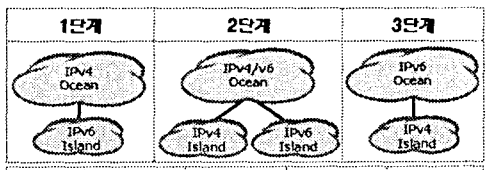
The BcN is applying from public networks to local networks and each terminal step by step until 2007. By IPv6 network introduction, IP address lack problem can be solved. However, the threats that network attacks of another method can be caused with new problem of network security in IPv6 networks. In this paper, we suggest the traffic analysis tool which analyze IPv6 traffic efficiently to detect/response network attack in IPv6 environment. The implemented IPv6 traffic analysis tool uses IPv6 header to analyze traffic and detect network attacks. Also, we also propose detection algorithm to detect network attacks in IPv6 networks.

키워드

네트워크 보안, IPv6, 공격 검출 알고리즘

I. 서 론

네트워크의 진화에 따라 2007년부터 국내 주요 ISP망에서 광대역통합망 (Broadband convergence Network: BcN) 환경이 구축될 예정이다. 또한, MIC에서는 네트워크 장비의 수명(약 5년)을 고려하여, 그림 1과 같은 과정을 거쳐 2005년부터 2009년까지 모든 공공기관 통신 장비를 순차적으로 업그레이드하고 2009년 이후에 IPv6가 단계적으로 공중망 및 지역망 단말에 도입될 할 것으로 예측하고 있다.



구 분	백본망	기입지망	단말기	비고
제1단계	IPv4	IPv4/IPv6	IPv4/IPv6	터널링 기술
제2단계	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6	Dual Stack
제3단계	IPv6	IPv6	IPv6	IPv6 전환

그림 1. IPv6 적용 단계[1]

본 논문에서는 IPv6 환경에서 발생 가능한 공격의 형태를 예상하여, 이러한 공격을 탐지할 수 있는 트래픽 분석 도구를 설계 및 구현한 내용을 다룬다.

II. IPv6 환경에서 예측 가능한 공격 방식

본 장에서는 IPv6 프로토콜의 취약점을 악용하여 발생할 수 있는 DAD-NA 메시지 공격, TCP SYN Flooding 공격, ICMP Flooding 공격, UDP Flooding 공격에 대해서 다룬다.

2.1 DAD-NA 메시지 공격

IPv6에서는 호스트가 자신의 MAC 주소와 라우터의 프리픽스를 이용하여 IPv6 주소를 자동으로 생성할 수 있다. 아래는 IPv6 주소 자동 생성 단계를 예시적으로 표현한 것이다.

1단계: 라우터로부터 서브넷 프리픽스를 얻음
서브넷 프리픽스: 12AB:0:0:CD30::/64
2단계: MAC 주소를 이용하여 64비트의 인터페이스 ID를 생성 00:40:2B:0E:0A:AD →
0240:2BFF:FE0E:0AAD
3단계: 서브넷 프리픽스와 인터페이스 ID를 결합하여 IPv6 주소 생성
IPv6 주소: 12AB:0:0:CD30:0240:2BFF:FE0E:0AAD/64

IPv6 주소는 수동으로 설정하거나 MAC 주소의 중복 또는 라우터 정책에 따른 주소 자동 설정 알고리즘에 의해 충돌할 가능성이 있다. 따라서, 비상태형 주소 자동 설정 방법에서는 DAD(Duplicate Address Detection)를 이용하여 동일한 네트워크상에 있는 호스트의 주소가 충돌하는지 여부를 검사한다.

DAD-NA(Neighbour Advertisement) 메시지 공격에서 공격자는 공격 대상 라우터의 내부에 에이전트를 설치한다. 에이전트는 NS(Neighbour Solicitation), NA 메시지를 이용하여 동일한 네트워크상에 있는 호스트들의 주소들을 수집하고, 수집한 주소들의 테이블을 이용해 공격자가 공격 명령을 지시하면 테이블에 있는 주소를 목적지 주소와 근원지 주소에 동일하게 넣고 NA 메시지를 보낸다. 같은 주소를 가지고 있는 호스트는 NA 메시지를 받았으므로 주소 충돌이라고 인식하게 된다[2]. 주소 충돌을 감지한 호스트는 주소 자동 재설정을 실행하는데 이때 라우터와 RA(Router Advertisement), RS(Router Solicitation) 메시지를 이용해 네트워크의 프리픽스 및 기타 주소 설정에 필요한 정보를 가져와 새 주소를 설정한다[3].

만약 라우터 내부에 있는 호스트의 주소가 많으면 많을수록 동시 다발적으로 발생하는 RS, RA 메시지 역시 증가하므로 결국 라우터로 많은 트래픽이 집중되면서 성능 저하를 발생시킨다[4].

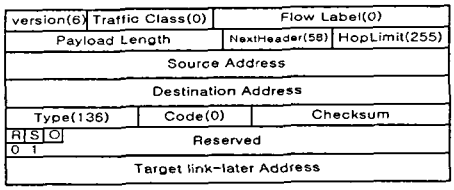


그림 2. DAD-NA 메시지 공격 헤더

2.2 TCP SYN Flooding 공격

TCP SYN Flooding 공격은 TCP 연결 설정의 취약점을 이용한 공격으로서, 악의적인 공격자가 SYN 메시지를 전송하고 SYN+ACK 메시지를 받은 후에 고의적으로 ACK를 보내지 않는 형태의 공격이다. 상대편 호스트는 ACK 메시지가 도착할 것으로 생각하고 반 오픈 상태가 되어 일정시간(75초) 동안 대기 상태에서 ACK 메시지를 기다린 후 다음 요청이 오지 않으면 해당 연결을 초기화하게 된다[5].

이처럼 지속적인 연결 요청을 수행한 후 다음 요청을 수락할 때까지 확인 메시지를 보내지 않으면 시스템에서 초기화되기 전까지 메모리 공간인 백로그 큐에 계속 쌓아두게 된다. 따라서 초기화하기 전에 계속적으로 새로운 요청이 오면 백로그 큐가 모두 차게 되어 더 이상 정상적인 연결 조차도 받아들일 수 없는 서비스 거부 상태가 된다.

TCP SYN Flooding 공격은 Next Header의 값을 6으로 설정한 후 근원지 주소를 위조하고, TCP 헤더의 Flag 필드에서 SYN 비트를 1로 세팅하여 지속적으로 전송하여 목표 시스템이 과부하로 인해 정상적인 서비스를 제공할 수 없도록 한다[6].

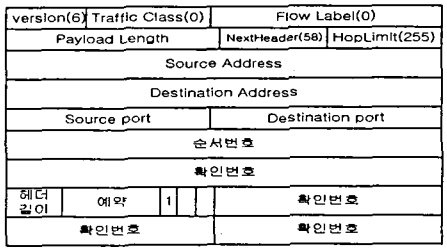


그림 3. TCP SYN Flooding 공격 헤더

2.3 ICMP Flooding 공격

ICMP Flooding 공격은 다량의 echo request 메시지를 보내서 목표 시스템을 정지시키는 공격으로, 목표 시스템에 대해 IP 주소 이외에는 추가적인 정보가 요구되지 않는 간단한 수법의 공격 방식이다.

또한 ICMP 요청 메시지를 브로드캐스트 주소로 보내게 되면 모든 시스템이 echo reply 메시지를 근원지 주소로 동시에 보내게 되어 해당 시스템이 다운되는 공격이다.

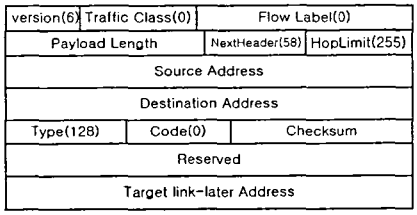


그림 4. ICMP Flooding 공격 헤더

2.4 UDP Flooding 공격

UDP Flooding 공격은 목적지의 포트번호 필드를 7, 31335, 19 등 특정 포트 번호로 세팅하고 서브넷의 브로드캐스트 주소를 목적지 주소로 하여 전송하는 형태의 공격이다. 이러한 공격은 UDP 데이터그램과 변형된 소스 IP 주소로 구성되어 있다.

단순한 TCP/IP 서비스를 수행하는 윈도우 NT 컴퓨터는 각각의 브로드캐스트에 모두 응답하는데, 그 양이 많을 경우 UDP 데이터그램의 Flooding 상태가 발생하게 된다.

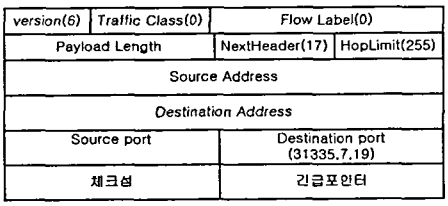


그림 5. UDP Flooding 공격 헤더

III. IPv6 트래픽 분석 도구 설계

본 논문에서 제안하는 IPv6 트래픽 분석 도구는 X윈도우 기반의 리눅스에서 개발된 것으로서, 아직 트래픽 분석은 로컬 네트워크로 한정하고 있다.

제안하는 IPv6 트래픽 분석 도구는 다음과 같은 방식을 통해서 네트워크 공격을 탐지한다.

- 공격자가 IPv6 환경에서 예상 가능한 유해 트래픽을 전송한다.
- 패킷이 경유하는 라우터에서 트래픽에 대한 정보를 수집한다.
- 헤더 정보를 분석하여 추정 공격 시나리오와 비교한다.
- 추정 공격과 같으면, 2차 판별을 수행한다.
- 공격으로 판단되면 경고 메시지를 콘솔에 보내고, 근원지 주소를 차단한다.

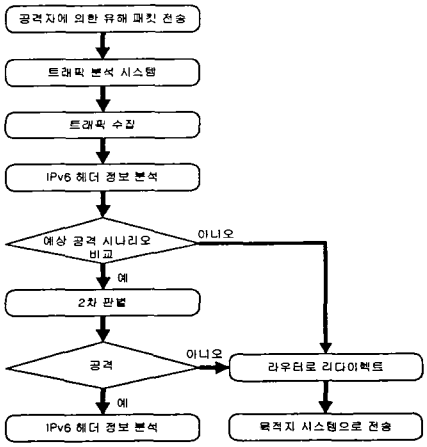


그림 6. IPv6 기반 트래픽 분석 도구의 흐름도

```
generate_module_start
  {
    while [ attack_packet-- >0 ]
     {
       a packet generate
       sleep interval
     }
  }

Packet_Capture_module_start
  {
    start Pcap library
    Pcaploop
     {
      store to packet.dat , IPv6save[]
      display one list to main window of program
      }
  }

Call Display_module

Display_module
  {
     create main window
     while(0)
      {
        call Detect_module
        display detection_result to sub windows
        }
  }

Detect_module
  {
     count each variable with IPv6 save[ ]
     make application of Detection algorithm
     store detection_result
   }
```

그림 7. IPv6 기반 트래픽 분석 도구의 전체 알고리즘

제안하는 IPv6 트래픽 분석 도구는 패킷 생성 모듈, 패킷 수집 모듈, 판별 모듈, X 윈도우 기반 디스플레이 모듈로 구성되어 있다.

패킷 생성 모듈은 2장에서 기술한 헤더를 갖는 공격 패킷을 생성하여 전송하는 공격자 역할의 모듈이며, 임의의 패킷을 생성하여 목표 시스템으로 유해 트래픽을 전송하는 기능을 수행한다.

패킷 수집 모듈은 패킷 생성 모듈로부터 전송된 패킷 및 지나가는 모든 패킷을 수집한다. 패킷 수집 모듈은 패킷을 수집하기 위한 환경 설정 및 패킷 필터링을 위한 설정 후 패킷 수신을 대기한다. 패킷 수집 모듈은 대기 모드에 있다가 패킷이 수집되면 수집된 패킷의 시간, 프로토콜, 근원지 IP 주소, 목적지 IP 주소, 필드 값을 구분하여 저장한다.

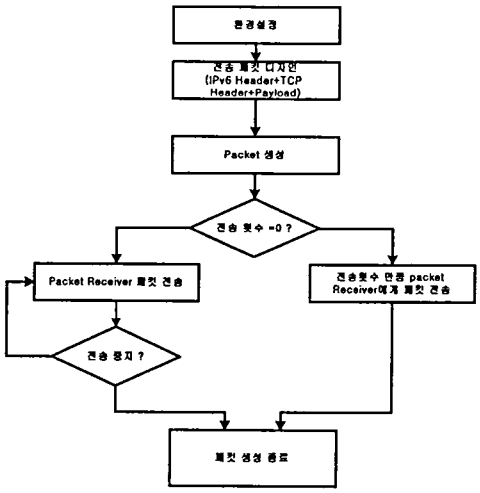


그림 8. 패킷 생성 모듈의 흐름도

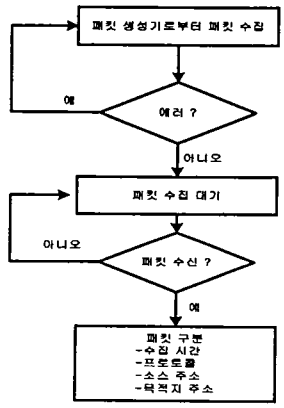


그림 9. 패킷 수집 모듈의 흐름도

판별 모듈은 패킷 수집 모듈에 의해 구분된 데이터를 근거로 공격 여부를 판정하는 역할을 한다. 추정한 공격들과 비교하여 일치하면 공격으로 간주하고, 일치하지 않으면 다시 한번 패킷을 검사한 후 정상으로 판정한다. 판별 데이터를 정상 패킷과 공격 패킷으로 구분하여 수집 시간, 프로토콜, 공격 유형, 근원지 주소를 저장한다.

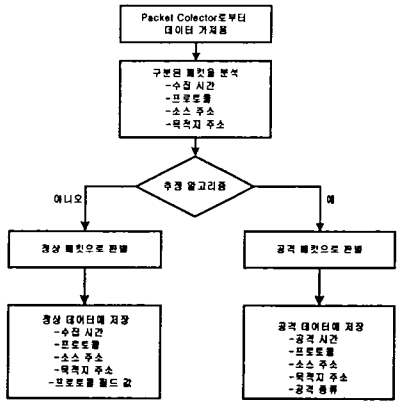


그림 10. 판별 모듈의 흐름도

X 윈도우 기반 디스플레이 모듈은 판별 모듈이 판정한 데이터를 이용하여 리눅스 시스템에서 GUI로 나타내는 역할을 한다. 공격이 검출되면 시스템 관리자에게 공격 알람 통보를 하고, 공격 헤더를 화면에 나타내며, 정상 패킷인 경우에는 단순히 프로토콜의 헤더만 보여준다.

V. 결 론

본 논문에서는 IPv6 도입을 고려하여 IPv6 네트워크 환경에서 발생할 수 있는 공격 방식에 대해서 분석하고, 이를 트래픽 분석을 통해 탐지할 수 있는 IPv6 트래픽 분석 도구를 설계하였다.

본 논문의 도구를 통해서 DAD-NA 메시지 공격, TCP SYN Flooding 공격, ICMP Flooding 공격,UDP Flooding 공격을 탐지할 수 있다. 향후에는 제시한 공격 이외의 다른 공격까지 탐지할 수 있도록 공격 탐지 알고리즘을 추가할 예정이다.

참고문헌

[1] 김선영, 오승희, et. al., "IPv6 기반 트래픽 분석 도구 설계", 한국콘텐츠학회논문지 Vol. 5, No. 2, p115~121, 2005. 4.

[2] Neighbor Discovery for IPv6, RFC 2461, 1998.

[3] Transition Mechanism for IPv6 Hosts and Routers, RFC 2993, 2003.

[4] Connection of IPv6 Domains via Clouds, RFC 3056, 2001.

[5] W. Stevens, TCP/IP Illustrated, Addison-Wesley, 1994.

[6] W. Stevens, Unix Network Programming, Prentice Hall, 1999.40, 2003