IPv6 환경의 보안 취약성 및 대응방안 분석

김영화, 김정태
목원대학교

Analyses of Security Vulnerability and Countermeasure in IPv6

Young-Hwa Kim, Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

Abstract

유비쿼터스 환경 구축에 필수적인 IP의 고갈은 이미 심각한 문제로 대두된지 오래며, IPv6의 도입 연구 및 시범적용이 활발이 진행되고 있어 거의 무한에 가까운 IP로 희망에 가득찬 u-Korea 건설을 목표로 순차적인 진행 단계에 있으나, 기존 IPv4 체계에서 IPv6 환경으로의 전환 및 프로토콜 스펙 변경으로 인한 보안에 대한 필요성 또한 증대되고 있다. 본 고에서는 IPv6 환경의 보안 취약성 및 이에 대한 대응방안의 분석을 통하여 이러한 보안 문제를 해결하기 위한 해법을 살펴보고자 한다.

1. 서론

인터넷의 빠른 발전과 통신/방송의 융합, 유/무선 통합, BcN, 홈네트워크 서비스와 같은 새로운 서비스의 필요성 증대 및 PC 뿐만 아니라 휴대전화, TV, 게임기, 카 네비게이션 등과 같은 수많은 정보기기들 간의 제어 및 소통을 위한 정보교환을 위하여 IP 주소의 소요가 증대되고 있다. 2022년 기존의 IPv4 주소는 수량의 한계와 더불어 운영상의 비효율로 인하여 완전고갈이 예상되며, 이를 대체하기 위하여 각 나라별로 국가별 차원의 전략이 수립되어 진행중에 있으며, 우리나라도 정부차원에서 IT839 전략에 의해 IPv6의 도입을 2010년까지 완료하여 ALL-IPv6 기반 서비스를 제공할 예정이며[2], 서울시의 경우 올해부터 Cisco 라우터를 이용하여 시범망을 구축하여 6개 기관에 대하여 IPv6 기반 시범서비스를 진행중이다.[3] IPv6는 기존 IPv4의 한계와 단점을 극복하고자 설계된 차세대 인터넷 표준으로 현재 많은 시제품들과 상용제품에서 탑재되고 있다. 특히, 윈도, 리눅스, BSD, 솔라리스 등의 운영체제들은 이미 IPv6 프로토콜을 지원하고 있다. 하지만 스위치나 라우터들의 IPv6 지원은 많이 진척되지 않고 있어 인터넷 서비스업체(ISP)들은 본격적으로 상용 IPv6 네트워크 서비스를 제공하고 있진 않다. 하지만, 궁극적으로 IPv4 주소 공간의 부족으로 인하여 IPv6로 전환해야 하기 때문에 IPv6 지원은 그리 멀지 않은 것으로 예측된다. 인터넷이 IPv6로 전환될 경우 현재 많이 발생하고 있는 인터넷 침해사고에 대한 대비책이 필요하다. IPv6는 IPv4와 달리 IPSec 프로토콜을 의무화하여 IP 프로토콜 자체의 보안성을 향상시켜 패킷의 무결성 및 기밀성을 충분히 제공할 수 있으나, 현재의 유동적이고 개방적인 현대의 네트워크를 고려할 때 IP 프로토콜 계층과 별도로 전송계층 또는 다양한 응용계층에서의 취약점으로 인하여 IPv6로 전환이 되는 차세대 인터넷에서의 침해사고는 IPv4와 크게 다르지 않을 것으로 예상된다. 본 논문에서는 우선 IPv6 프로토콜의 새로운 기능에 대한 보안 취약성, IPv4에서 IPv6로의 전환기술과 관련된 보안 취약성과 그리고 IPv4 및 IPv6 네트워크 환경에서 공통적으로 나타날 수 있는 보안 취약성 및 이에 대한 대응방안에 대하여 알아본다.

2. IPv6의 보안취약성 및 대응방안

패킷의 무결성 및 기밀성은 IPv6상에서 기본적으로 제공하는 IPSec을 이용하여 충분히 제공해 줄 있으나, 현재의 네트워크는 IPv6의 도입으로 인한 예상치 못한 취약성을 만들어 내거나 악화시킬 수 있는 환경이고 이러한 환경에서 다음과 같은 보안 취약성이 있다.

- IPv6의 확장된 주소 범위로 인해 호스트를 찾기 위한 포트 스캐닝이 어렵다는 반면에 공격자를 추적하기 어려움
- 침입차단시스템과 침입탐지시스템은 IPv6의 새로운 기능 및 보안 기능 처리를 위한 CPU 오버헤드로 인해 서비스거부공격 가능성이 높음
- 라우팅 헤더 등의 확장 헤더를 악용하여 침입차단시스템을 우회할 수 있음
- 공격자는 IPv6 주소 자동설정 기능을 악용하여 정상적인 주소 할당을 방해하거나 정상적인 세션을 종료할 수 있음[5]

1) 라우팅 헤더

IPv6 라우팅 헤더는 패킷이 목적지까지 경유하는 중계 라우터들을 송신자가 지정하는데 사용된다. 침입차단시스템의 접근제어 규칙에 의해 공격자 A가 내부 서버 B에 접근이 가능하나, 내부 서버 C에는 접근할 수 없도록 설정되어 있을 경우 접근 가능한 내부 서버 B의 라우팅 헤더 처리가 가능하고 라우팅 헤더의 'Segments Left' 필드 값이 1 이상인 경우에 공격자 A는 내부 서버 B를 경유하여 내부 서버 C로 공격 트래픽을 전달할 수 있다. 따라서 라우팅 헤더를 이용하면 목적지 주소 기반의 접근 제어를 하는 침입차단시스템의 필터링을 우회할 수 있다.

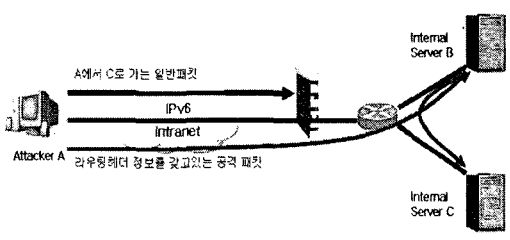

그림 1. 라우팅 헤더 보안 취약성

이에 대응하기 위하여 침입차단시스템은 type 필드 값이 0인 라우팅 헤더를 갖는 패킷을 차단하도록 필터링 규칙을 설정하고, 최종 목적지 주소와 라우팅 헤더의 'Address' 필드 값을 비교할 수 있는 필터링 규칙을 설정하며, 호스트는 수신된 패킷의 라우팅 헤더에 포함된 최종 목적지 주소가 자신의 주소가 아닌 경우에는 패킷을 폐기토록 설정하여야 한다.

2) 멀티캐스트 주소

IPv6에서는 브로드캐스트 주소 대신에 멀티캐스트 주소를 이용하여 브로드캐스트 서비스를 제공하며, 모든 라우터(FF05::2) 및 모든 DHCP서버(FF05::1:3)를 지정하는 주소 제공을 통하여 이를 목적지 주소로 사용하여 플러딩 공격(Flooding Attack)을 할 수 있다. 또한 IPv4 환경에서는 공격자가 취약한 시스템을 찾기위해 네트워커상의 (2^8=256)개 호스트들에 대해 무작위 스캔공격을 해야 하나 IPv6 환경에서는 최대 2^{64}개의 호스트들을 스캔해야 하므로 공격자는 범위를 줄이기 위해 다음과 같은 보안 취약성을 이용할 수 있다.

관리상의 이유로 각 노드들에 대해 기억하기 쉬운 주소를 사용 및 IEEE EUI-64 주소의 고정부분을 이용하여 작은 범위의 주소 공간에 대한 스캔으로 다른 노드들도 유추 가능하며, 이더넷 카드 제조 회사의 정보를 이용하여 인터페이스의 주소 범위 추측이 가능하다. 이러한 공격을 막기 위하여 외부로부터 멀티캐스트 주소에 접근할 수 없도록 네트워크 경계 지역의 침입차단시스템 및 침입탐지시스템에서 필터링을 수행하여야 한다.

3) ICMPv6

'Destination Unreachable' 에러 메시지는 목적지 노드에 도달할 수 없는 패킷에 대해 생성된다. 에러 메시지는 송신자가 속한 라우터 또는 목적지 노드에서 생성되며, 이러한 처리가 불가능한 특정 패킷들이 멀티캐스트 주소로 전송되면 에러 메시지를 송신자에게 보내는 것을 허용함으로써 다음과 같은 취약점을 갖는다. 수신한 패킷의 크기가 'next link MTU'도 다 큰 경우에는 멀티캐스트 트래픽에 대한

'Path MTU Discovery'를 지원하기 위해 'packet too big' 이라는 응답메시지를 전송함으로써 서비스거부공격에 취약하고, hop-by-hop 또는 Destination Option 확장헤더에 옵션값이 잘못 설정된 패킷을 수신할 경우에는 'parameter problem' 응답메시지를 전송함으로써 서비스거부공격에 취약하다. 또한, 공격자가 ICMPv6메시지 중 RS(Router Solicitation)와 RA(Router Advertisement)메시지를 위조하여 잘못된Prefix 정보를 내부 네트워크에 전파할 수 있다. 이에 대응하기 위하여 IPv6에서는 목적지나 목적포트에 대한 필터링뿐만 아니라 확장헤더에 대한 필터링이 가능하여야 하며, 침입차단시스템이 neighbor discovery protocol 및 neighbor solicitation protocol의 처리를 지원하고, 동적 라우팅 프로토콜을 필터링 할 수 있어야 하며, 다양한 인터페이스 타입을 지원할 수 있어야 한다.

4) 애니캐스트

애니캐스트 서비스에서 송신자의 요청은 애니캐스트 라우터를 통하여 짧은 홉거리, 낮은 비용, RTT 등을 고려하여 적합한 그룹의 멤버에게 전달되며, 이때 그룹 멤버는 응답 메시지의 소스주소를 글로벌 유니캐스트 주소로 변경하여 송신자에게 응답한다. 인증되지 않은 애니캐스트 그룹 멤버가 거짓 정보를 광고하거나 해당 멤버에 의해 송신자의 주소를 변경할 수 있는 보안취약성으로 인하여, 위장공격 및 서비스거부공격이 가능하다. 이에 대응하기 위하여 외부에서의 애니캐스트 서비스 요청을 제한하기 위해 침입차단시스템은 사용되는 애니캐스트 주소를 필터링을 하거나, IPSec 및 IKE(Internet Key Exchange Protocol)을 애니캐스트에 적용하여 보안통신채널을 사용해야 한다.

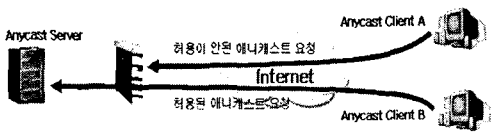

그림 2. 침입차단시스템을 이용한 패킷 필터링

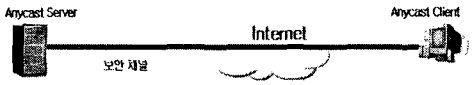

그림 3. 통신보안 채널 설정을 통한 통신

5) 프라이버시 확장

호스트가 주소를 할당받기 위해 수동설정이나 DHCP를 통하는 경우에는 DNS에 주소를 등록하는 것이 제한적이나 주소 자동설정을 이용하면 DDNS(Dynamic DNS)를 통해 동적으로 주소를 등록할 수 있다. 이로 인해 공격자가 자신의 주소를 용이하게 변경할 수 있어 분산서비스거부공격에 대한 방어가 어려울 수 있으며, 주소 자동설정에 프라이버시 확장을 사용하면 DDNS의 업데이트 작업의 오버헤드가 발생하여 가용성이 떨어질 수 있다. 이에 대응하기 위하여 주소 설정을 위한 노드와 DDNS 서버 간 SA(Security Association)를 통하여 인증된 노드만이 주소 갱신을 하도록 하며 프라이버시 확장을 사용하는 노드는 주소 업데이트 주기에 대한 적절한 값을 설정해야 한다.

3. IPv4/IPv6 공통 보안취약성 및 대응방안

IPv6에서의 보안 기능은 IETF에서 개발된 IPSec에 의해 지원되며, IPv6 기반 IPSec이 제공할 수 있는 보안서비스에는 접근제어, 무결성, 데이터 근원 인증, 재실행된 패킷 거부, 기밀성 등이 포함된다. 이러한 보안 서비스들은 IP 계층에서 제공되기 때문에 TCP, UDP, ICMP, BGP 등의 어떠한 상위 계층 프로토콜에 의해서도 사용될 수 있는 장점을 가지며, TCP/IP 통신을 보다 안전하게 유지하기 위한 종단간 암호화와 인증을 제공해 준다. IPSec은 트래픽 보안을 위해 AH 및 ESP 프로토콜을 사용한다. AH 프로토콜은 무결성, 데이터 근원 인증 및 선택적 재실행 방지 서비스를 제공하며, ESP 프로토콜은 기밀성을 제공할 수 있다.

<표 1> IPSec AH/ESP 프로토콜의 보안 서비스

보안서비스	AH	ESP
접근제어	○	○
비연결형 무결성	○	○
데이터 발신 인증	○	○
재전송 방지	○	○
비밀성		○
제한적 트래픽 흐름의 비밀성		○

AH(Authentication Header)는 IP 데이터그램을 인증하기 위해 필요한 정보를 포함하는 방법으로 보안 효과, 특히 데이터의 인증과 무결성을 보장해 주는 메커니즘이다. AH는 다음과 같은 보안서비스를 제공한다

- 데이터의 무결성 : 메시지 인증을 담당하는 코드(Message Authentication Code)에 의해 계산된 각 필드의 합산 값을 수신자가 확인
- 데이터의 인증 : 인증 시 필요한 키와 알고리즘을 SA(Security Association)와 연계하여 지정하고 지정된 알고리즘을 수행
- 재생공격 방지 : 인증헤더에 있는 Sequence Number 필드의 값을 일련 번호화 함

4. 결론

현재까지 사용되어 온 IPv4 프로토콜은 기본적으로 보안을 고려하여 설계되지 않았기 때문에, 다양한 보안 공격에 노출되어 있는 반면, IPv6에서는 IPSec을 기본으로 제공하는 등 보안이 상당히 강화되어 이제까지의 공격을 상당부분 해결할 수 있다. 그러나, IPv6에서 제공하는 자동설정, 확장헤더 등 새로운 기능과 IPv4에서 IPv6로의 전환시의 보안 취약성을 노린 공격이 새롭게 나타날 것이다.이렇듯 갈수록 지능화, 고도화되는 위협으로부터 네트워크를 안전하게 운용할 수 있는 보안기술 및 독자적인 보안시스템 개발은 필수적이며, IPv6 환경에서 발생 가능한 보안 취약성 과 대응방안에 대한 핵심기술의 확보가 필수적이다.

참고문헌

[1] IPv6 동향 2004, 정보통신부/한국전산원
[2] 2005 IPv6 동향, 정보통신부/한국전산원
[3] www.ipv6seoul.go.kr, 서울특별시 시범망 구축사업
[4] IPv6 보급 촉진 기본계획, 정보통신부
[5] IPv6 보안 기술 해설서, 한국정보보호진흥원
[6] http://cafe.naver.com/starvankorea/827
[7] IPv6 IPSec 기술 및 동향, Future Systems
[8] IPv6 Security Vulnerability and Countermeasures, IPv6 포럼코리아 제주 워크샵(2005)
[9] http://www.cisco.com, Implementing IPSecin IPv6
[10] http://www.ipv6life.com, IPv6 Intro
[11] 정보홍, 임재덕, 김영호, 김기영, "IPv6 환경의 보안 위협 및 공격 분석", 전자통신동향분석, 통권 103호, 2007, p.37-50
[12] 2006 정보시스템 해킹 · 바이러스 현황 및 대응, 한국정보보호진흥원