# IPv6 환경의 보안 위협 및 공격 분석

An Analysis of Security Threat and Network Attack in IPv6

u-IT839의 정보보호 이슈 특집

정보흥 (B.H. Jung) 보안운영체제연구팀 선임연구원
임재덕 (J.D. Lim) 보안운영체제연구팀 선임연구원
김영호 (Y.H. Kim) 보안운영체제연구팀 연구원
김기영 (K.Y. Kim) 보안운영체제연구팀 팀장

목 차



차세대 인터넷 표준인 IPv6가 제정되고 보급되기 시작하면서 IPv6에서의 보안이 중요한 이슈로 등장하고 있다. IPv6는 기존의 IPv4와 달리 IPsec을 기본적으로 지원하여 보안성이 강화될 것으로 예상하고 있으나 IPv6 환경으로의 전환, IPv6 프로토콜 스펙의 변경 등의 요인으로 인하여 보안에 대한 필요성이 증대되고 있다. 본 고에서는 IPv6 환경의 보안위협 및 공격들을 분석하고 침입탐지/차단 기술의 관점에서 이러한 보안 문제를 해결하기 위한 방법을 기술한다.

# I. 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 네비게이터 등과 같은 수많은 정보기기들 간의 정보 교환을 위하여 IP 주소의 수요가 증대되고 있다. 이에 따라 IPv4 환경에서 사용될 수 있는 IP 주소가 부족하게 되는 현상이 발생하게 되고, 전문가들의 예측에 의하면 IPv4 주소는 2022년이면 완전히 고갈될 것으로 예측되고 있다. 이를 위해 미국, 일본, 유럽 등에서는 지난 2000년부터 IPv6 도입을 위한 국가적 차원의 전략을 수립해 본격적인 보급 및 활성화 작업을 추진하고 있다. 특히, 미국은 세계에서 가장 먼저 IPv6 지원 라우터 장비를 상용화하였고, 2005년 4월에는 "Coalition Summit for IPv6"를 통하여 경찰, 병원, 소방서 등 긴급 에이전시에 IPv6 기반 긴급 관리시스템을 도입하는 "Metronnet6" 프로젝트를 발표할 정도로 구체적인 보급정책을 추진하고 있다. 국내에서는 정부차원에서 IT839 전략에 의해 IPv6의 조기 보급 확산을 위해 IPv6 기반 시범서비스(WiBro, VoIP, 홈네트워크 등)를 추진중이다[1].

IPv6는 IPv4의 단점을 극복하고자 설계된 차세대 인터넷 표준으로 2006년 현재 많은 시제품들과 상용제품에서 탑재되고 있다. 특히, 윈도, 리눅스, BSD, 솔리리스 등의 운영체제들은 이미 IPv6 프로토콜을 지원하고 있다. 하지만, 스위치나 라우터들의 IPv6 지원은 많이 진척되지 않고 있어 인터넷서비스업체(ISP)들은 본격적으로 상용 IPv6 네트워크 서비스를 제공하고 있지 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 침해 사고에 대한 대비책이 필요하다. IPv6는 IPv4와 달리 IPsec 프로토콜을 의무화하여 IP 프로토콜 자체의 보안성을 향상시켰다. 하지만, IP 프로토콜 계층과 별도로 전송계층 또는 다양한 응용계층에서의 취약점으로 인하여 IPv6로 전환이 되는 차세대 인터넷에서의 침해사고는 IPv4와 크게 다르지 않을 것으로 예상된다. 더욱이, IPv4/IPv6 전환 시에는 많은 IPv4 네트워크 장비들이 의도하지 않게 IPv6 트래픽을 통과시킬 수 있어 오히려 인터넷 침해 사고의 위험이 증가할 수도 있다. 이미 해커들에 의해서 IPv6 프로토콜이 악용된 사례도 보고되고 있다. 또한, 최근 IETF 내의 보안 그룹 등에서 IPv6 프로토콜에서의 확장헤더의 사용, IPv4/IPv6 전환 메커니즘 사용시 보안 문제가 발생할 수 있다고 연구결과를 발표하고, 이에 대한 보안 확인을 반드시 하도록 권고하고 있다.

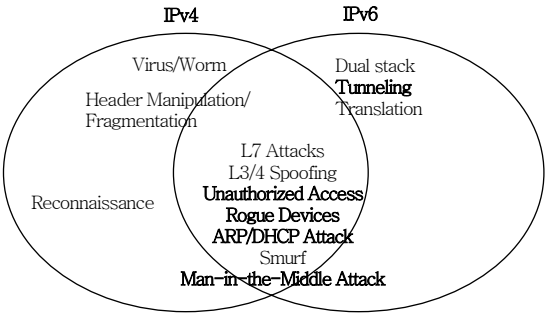
현재 IPv6 네트워크에서의 인터넷 침해대응을 위한 도구의 개발은 미미한 실정이며, SNMP, RMON, Cisco NetFlow[2] 등은 부분적으로 IPv6를 제공하고 있고, 많은 방화벽/IDS/IPS 등의 네트워크 보안 제품들 역시 IPv6 기능을 본격적으로 제공하고 있지는 않다. 따라서, 본 고에서는 IPv6에서의 보안 위협 및 취약성에 대해 알아보고 이를 해결하기 위한 IPv6 침입탐지 및 차단 기술에 대해 설명한다.

**● 용 어 해 설 ●**

IPv6: IPv6는 인터넷 국제표준화 기구인 IETF IPv6 워킹그룹에서 1988년부터 표준화 작업을 시작한 차세대 IP 프로토콜로서, 현재 사용되고 있는 IP 프로토콜인 IPv6를 대신할 예정임.

# Ⅱ. IPv6로 전환시 보안 위협

IPv6 환경으로 전환시 나타날 수 있는 보안 위협은 (그림 1)에서와 같이 IPv4에서 존재하였던 위협 요소뿐만 아니라 IPv6에서 새로이 나타날 위협 요소를 포함하여 복합적으로 나타날 수 있다. IPv6 주소공간이 128비트로 확장되어 스캐닝이나 이를 이용하는 웜과 같은 것들은 IPv6에서 대폭 감소될 것으로 예상되고 있다. 하지만, IPv4에서 IPv6로 전환하는 기술인 터널링이나 듀얼 스택과 같은 것들이 보안의 취약점으로 작용할 수 있다.




(그림 1) IPv4/IPv6에서의 보안 위협 요소

IPv6에서 가능한 공격이나 위협 요소들은 다음과 같다.

1) 사전공격(Reconnaissance)

스캐닝 또는 검색엔진 및 공개된 문서 등의 데이터 마이닝을 통한 사전공격들로서 공격자가 공격을 하기 전에 다양한 방법을 통하여 탐색하는 과정이다. IPv4에서는 ping sweep, port scan 및 응용 취약점 스캔 등에 관련된 다양한 툴들이 알려져 있다. IPv6에서는 ping sweep, port scan과 같은 스캔 트래픽은 IPv6에서는 거의 불가능해진다. 왜냐하면, IPv4의 디폴트 서브넷 크기인 8비트에서는 28개의 스캔이면 충분하지만, IPv6 디폴트 서브넷 크기인 64비트에서는 264개의 스캔을 해야 한다. 게다가, IPv6 주소는 MAC 주소의 EUI-64 버전을 사용하기 때문에 랜덤한 주소를 가지게 된다. 하지만, DNS 또는 일반 호스트를 위한 동적 DNS를 통해 서브넷에 가능한 주소를 쉽게 알 수도 있다. 한편으로 IPv6에서는 멀티캐스트 주소 사용이 많아지게 되어 중요한 네트워크 자원들(라우터, DHCP 서버, NTP 서버)이 쉽게 노출될 수 있다.

2) 권한없는 접근(Unauthorized access)

IPv4에서는 접근 제어 리스트(ACL)를 통해서 3계층 또는 4계층의 접근에 관한 정책이 게이트웨이 형태의 방화벽이나 종단 호스트에서의 방화벽으로 구현된다. IPv6에서는 IPsec이 AH만 사용된다면, 상위 프로토콜의 내용에 대해서 조사할 수 있다. IPv4 헤더의 옵션은 IPv6에서 확장 헤더로 변경되었다. 그런데, 이 확장 헤더에는 라우팅 옵션과 같이 종단 호스트가 처리한 후 다시 패킷을 전송할 수도 있다. 특히, MIPv6에서 이러한 문제가 발생할 수 있으므로 어떤 호스트가 홈 에이전트(home agent)로 동작할지 미리 설정해두어야 한다. 그리고, ICMPv6는 IPv6에 포함되었기 때문에 방화벽 설정시 좀더 많은 점들이 고려되어야 한다. 방화벽 자체에 대한 메시지로는 ICMPv6 type 2, ICMPv6 type 130-132, ICMPv6 type 133/134, ICMPv6 type 135/136, ICMPv6 type 4 등이 지원되어야 한다. 멀티캐스트 주소는 IPv6에서 자주 사용되기 때문에 링크-로컬 멀티캐스트 주소 허용을 최소화해야 한다. DNS나 NTP 서버에 대한 애니캐스트 주소도 IPv6에서 사용되기 때문에 이에 대한 조사도 지원되어야 한다.

3) 헤더 조작과 단편화(Header manipulation and fragmentation)

IPv4 단편화는 NIDS나 방화벽을 우회시킬 수 있는 방법으로 이용되었기 때문에 대부분의 방화벽이나 NIDS에서는 단편들을 재조립해서 검사하는 기능이 필수적이다. IPv6에서 중간노드들에 의한 단편화는 금지되어 있다. IPv4에서의 공격으로 인한 파편들을 중첩시키는 방법이 흔하게 사용될 수 있는데, 이 역시 제한되어야 하고 RFC2460에서 정의된 IPv6 최소 MTU 크기인 1280바이트 이하의 패킷들(마지막 패킷 제외) 역시 제한되어야 한다.

4) 3계층과 4계층 위장(Layer 3/4 spoofing)

IPv4에서는 DoS, 스팸, 웜 등의 공격에서 흔히 IP 주소 위장 방법이 사용된다. RFC2827에서는 인그레스 필터링(ingress filtering) 방법으로 이러한 주소 위장 공격을 차단시키는 방법을 제안하고 있다. IPv6 주소는 요약이 되도록 할당되기 때문에 RFC2827과 같은 인그레스 필터링이 구현될 수 있다. 하지만, 서브넷 크기가 크고, IPv4에서 IPv6로 변환될 때 6to4 터널링과 같은 방법이 사용될 수 있기 때문에 여전히 주소 위장 방법이 위협이 될 수 있다.

5) ARP와 DHCP

IPv4에서는 DHCP의 경우 브로드캐스트를 사용하므로 위장 DHCP 서버가 가짜 응답을 전송할 수 있다. 그리고, ARP 공격을 통해서 IP-MAC 주소 바인딩 정보를 변경시킬 수 있다. IPv6에서는 stateless 주소자동설정 방법이 사용되지만, 부가적인 보안장치는 되어 있지 않다. 여전히 stateless 주소자동설정 메시지가 위장될 수 있다는 것이고, "신뢰하는 포트"의 방법과 같은 것들이 구현되어야 한다. ARP는 IPv6에서 ICMPv6 기능의 일부인 ND로 변경되었다. IETF SEND 워킹 그룹에서 이러한 문제를 다루고 있다.

6) 브로드캐스트 증폭 공격(Broadcast amplification attacks: smurf)

IPv4에서는 IPv4 directed broadcast를 라우터에서 제한하도록 하여 서브넷으로 향했다가 가짜 송신자 주소로 되돌아가는 공격 트래픽을 막을 수 있다. IPv6에서는 IP-directed broadcast의 개념이 없다. RFC2463에서는 구체적으로 IPv6 멀티캐스트 주소로 향하는 트래픽에 대하여 ICMPv6 응답 메시지가 생성되지 않도록 하고 있다. 따라서, 표준대로 구현된다면 스머프 공격이 제대로 이루어지지 않는다. 글로벌 멀티캐스트 주소가 송신자일 경우에 ICMP 응답을 보내야 하는지에 대해서는 아직 표준에서 논의중이다.

7) 라우팅 공격(Routing attacks)

라우터에 대한 공격으로 플러딩이나 경로를 임의로 알리거나 교체하도록 하여 트래픽의 흐름을 엉뚱하게 하거나 막도록 하는 것이다. IPv4에서는 MD5나 키 교환 등의 암호화된 인증 방식을 통하여 안전하게 경로를 알리도록 하고 있다. IPv6에서는 BGP는 TCP MD5로 인증을 하고 있고, IS-IS에서는 RFC3567을 통하여 암호화된 인증 방식을 사용하고, OSPFv3와 RIPng에서는 자체 인증 필드는 삭제한 반면 IPsec AH/ESP를 사용하고 있다.

8) 바이러스와 웜

바이러스와 웜 자체는 IPv6에서도 여전히 위해요소이지만, IPv6 주소 공간의 크기 변화로 인하여 스캐닝이 거의 불가능해지기 때문에 바이러스와 웜의 파괴력이 떨어진다.

9) 번역, 전환 및 터널링 메커니즘

자동 터널링과 같은 방법은 패킷 위장 및 DoS 공격을 가능하게 하기 때문에 이러한 패킷들에 대한 조사 부담이 추가된다.

10) 스니핑(Sniffing)

전송되는 데이터를 캡처하는 공격으로 IPv6에서는 IPsec이 디폴트로 제공되어 원천적으로 차단될 수 있다. 하지만, 복잡한 키 분배의 문제점으로 인하여 IPsec의 보급이 더디게 된다면 여전히 문제가 될 수 있다.

11) 응용 계층 공격

버퍼 오버플로, 웹 응용 공격, 바이러스 및 웜 등은 IPv4와 IPv6 환경에서도 동일한 문제이다.

12) 악의적 디바이스(Rogue devices)

네트워크에 권한없이 연결되어 있는 디바이스로 무선 액세스 포인트, DHCP, DNS 서버, 라우터 및 스위치 등이 될 수 있다. IPsec을 통한 인증이 강화된다면 이러한 문제가 줄어들 것이다.

13) Man-in-the-middle 공격

IPv4 및 IPv6 헤더에는 자체적으로 보안 기능이 없다. 따라서, IPsec을 사용하는 데 IKE의 공격을 이용한 공격이 가능하다. IKEv2에서는 이러한 문제를 보완하고 있다.

14) 플러딩

플러딩 공격과 역추적 메커니즘은 IPv4와 IPv6 동일하게 적용된다.

## Ⅲ. IPv6 침입탐지 및 차단을 위한 보안 고려사항

IPv6 환경에서는 기존의 IPv4 환경과는 다르게 IPv6 프로토콜에 새로이 등장하는 특징으로 인한 취약점이 존재하여 IPv6 환경에서의 침입탐지 및 차단을 위해서는 다음의 보안위협요소에 대한 고려가 필요하다.

### 1. IPsec 관련 보안 고려사항

IPsec 관련 보안 고려사항으로는 키 교환 메커니즘과 관련한 성능 저하 문제와 ESP 트래픽과 관련한 보안정책 적용 문제가 있다. ESP 트래픽과 관련한 보안 정책 적용 문제로는, AH 트래픽과 달리 ESP에 의해 암호화된 IPv6 패킷은 소스/목적지 호스트 이외의 다른 호스트에서 내용을 해석할 수 없을 뿐만 아니라 터널 모드의 경우 최종 목적지 호스트조차 알 수 없기 때문에 공격자에게 해당 패킷이 악용되거나 내용이 노출되는 것을 최대한 줄일 수 있다. 그러나 패킷 전달 경로 중간에 위치한 노드들은 ESP 트래픽의 운영 모드(전송 모드와 터널 모드)에 상관없이 전송 계층 이상의 패킷 내용을 확인할 수 없기 때문에 패킷 내용의 신뢰성 또한 검증할 수 없다. ESP 트래픽을 중간 노드에서 검사할 수 없는 것은 해당 패킷에 방화벽과 같은 패킷 검사를 수행하는 보안 장비의 정책을 적용할 수 없음을 의미한다. 암호화된 트래픽을 검사할 수 있는 방법이 존재하지 않기 때문에 방화벽과 같은 보안 장비에서 암호화된 트래픽을 모두 통과시키는 정책을 적용한다면 공격자는 이를 악용하여 임의로 암호화된 패킷을 전송함으로써 방화벽을 우회하는 공격을 시도할 수도 있다.

### 2. 프라이버시 및 DAD 관련 보안 고려사항

RFC2462 IPv6 Stateless Address Auto-configuration에 정의된 바와 같이 stateless 주소 자동 설정 메커니즘은 IPv6에서 새롭게 추가된 가장 중요한 메커니즘 중의 하나로서 로컬 링크상의 모든 노드들은 라우터가 전송하는 네트워크 프리픽스 정보와 로컬 인터페이스 카드 ID를 이용하여 자신의 IPv6 주소를 생성하도록 권고한다. 그러나 로컬 인터페이스 카드 ID를 IPv6 주소를 생성하는 데 이용하는 것은 여러 보안 관련 문제를 발생시킬 수 있다.

#### 가. 프라이버시 문제

자동 주소 설정에 사용되는 인터페이스 주소에는 사용중인 기기의 종류를 판별할 수 있는 식별 값, 제조사, 모델번호 등이 포함되어 있기 때문에 IPv6 주소를 통해 사용자의 의사와 상관없이 공격자에게 사용중인 하드웨어의 특정 정보를 제공하는 데 쓰일 가능성이 존재한다. IPv6 주소의 하드웨어 ID 부분을 이용하여 네트워크에 존재하는 각 장치들의 활동을 추적할 수 있다.

#### 나. DAD를 악용한 서비스거부공격의 가능성

자동 주소 설정 기능을 이용하여 IPv6 주소를 생성하는 모든 노드들은 DAD 메커니즘을 이용하여 주소의 유효성 여부를 검증받아야 한다. 일반적으로 부팅시 자동으로 가장 먼저 생성되는 링크 로컬 주소를 검증하기 위하여 DAD가 처음으로 실행된다. 만약 링크 로컬 주소의 DAD 검사가 통과하면 이후 동일 인터페이스 카드 ID로 생성되는 다른 IPv6 주소는 DAD 검사를 수행할 필요 없이 유일함을 보장받는다. RFC2462에서는 할당된 IPv6 주소가 DAD 검사에 실패했을 때 그 주소를 사용할 수 없음을 명시하고 있다[3]. 이를 악용하여 사용자는 DAD 검사가 실패하도록 계속해서 고의적인 메시지를 전송함으로써 서비스거부 공격을 발생시킬 수 있다.

### 3. ND 메커니즘 관련 보안 고려사항

RFC2461과 2462에 정의되어 있는 IPv6 ND 메커니즘과 주소 자동 설정 메커니즘은 RFC2461의

Neighbor Discovery for IP Version 6에 정의된 바와 같이 IPv6 프로토콜에서 매우 중요한 구성요소이다[3]-[5]. ND는 ARP 대체 기능의 수행 및 stateless 주소 자동 설정 메커니즘에 관여한다.

### 가. 라우터/라우팅 메커니즘과 관련 없는 공격

#### 1) NS/NA 메시지 위장 공격

악의적인 사용자는 IPv4의 ARP 스푸핑 공격과 유사하게 NS/NA 메시지 내의 source link-layer 옵션과 target link-layer 옵션에 저장될 링크 계층 주소를 조작하여 이 메시지를 수신한 노드들이 해당 메시지에 저장된 링크 계층 주소를 기반으로 네이버 캐시 엔트리를 변경하도록 유도할 수 있다. 이를 통해서 패킷 전달 경로를 우회하도록 만들 수 있다.

#### 2) NUD 실패 유도 공격

NUD 메커니즘은 악의적인 사용자가 자신의 공격을 계속해서 유효한 상태로 만드는 데 악용될 수 있다. 즉 NS/NA 위장 공격에서 설명한 것처럼 공격자는 링크 상에 존재하지 않는 주소로 victim 호스트의 네이버 캐시 엔트리를 생성하도록 할 수 있으며, 이 경우 victim 호스트는 해당 패킷이 존재하지 않는 호스트로 전달되어 어떠한 응답 패킷도 받을 수 없는 상태가 되기 때문에 NUD 메커니즘을 수행하게 된다. 정상적인 경우 NUD 과정은 실패하게 되기 때문에 victim 호스트에 불법으로 생성된 네이버 캐시 엔트리는 삭제될 것이다. 그러나 공격자는 victim 호스트가 수행하는 NUD 과정에 개입하여 또 다시 링크 계층 주소가 위장된 NA 패킷으로 응답함으로써 NS/NA 메시지 위장 공격이 계속해서 유효한 상태로 유지되도록 유도할 수 있다.

### 나. 라우터/라우팅 메커니즘 관련 공격

#### 1) 라우터 위장 공격

공격 호스트는 로컬 링크 상의 노드들에게 위장된 패킷을 전송함으로써 자신이 네트워크 내의 라우터인 것처럼 위장할 수 있다. 네트워크 내의 호스트들이 공격 호스트를 디폴트 라우터로 설정하도록 함으로써 전송되는 모든 트래픽이 공격 호스트로 우회하여 전달되도록 한다. 이는 패킷 전달 경로 우회 공격에 해당된다. 만약 공격 호스트가 해당 트래픽을 중간에서 모두 차단한다면 노드들의 정상적인 패킷 전송이 불가능해지기 때문에 서비스 거부 공격을 유발하는 데 악용될 수도 있다.

#### 2) 디폴트 라우터 삭제 공격

RFC2461에 의하면 IPv6에서는 노드의 디폴트 라우터 리스트에 등록된 라우터가 한 개도 존재하지 않을 경우 자신이 속한 네트워크에서 패킷을 전송할 때 라우터가 필요하지 않은 것으로 인식하기 때문에 모든 노드들이 1홉 내의 on-link 상에 존재한다고 간주한다. 공격자는 위 사실을 악용하여 서비스거부 공격을 수행한 후 노드의 디폴트 라우터 리스트에 어떠한 엔트리도 존재하지 않도록 만듦으로써 victim 호스트들이 자신이 통신하고자 하는 모든 노드가 on-link 상에 존재하는 것처럼 착각하도록 유도할 수 있다.

#### 3) 리다이렉트 메시지 위장 공격

일반적으로 호스트들은 라우터로부터 리다이렉트 메시지를 받았을 경우 해당 메시지의 소스 주소가 자신이 메시지를 전송했던 라우터의 링크 로컬 주소와 일치하는지의 여부를 검사하여 해당 메시지의 유효성 여부를 검사한다. 즉 받은 리다이렉트 메시지의 소스 주소가 전송된 메시지의 목적지 주소(라우터 링크 로컬 주소)와 일치한다면 해당 리다이렉트 메시지는 유효한 것으로 간주된다. 패킷내용 변조에 대한 검증절차가 없기 때문에 이를 악용한 리다이렉트 메시지 위장 공격이 가능하다.

#### 4) On-link 프리픽스 위장 공격

일반적으로 RA 메시지의 프리픽스 주소 옵션에 on-link 플래그 값이 1로 설정되어 있다면 이는 해당 메시지를 통하여 전달되는 프리픽스 주소 범위에

속한 호스트들이 1홉 내의 링크 로컬 상에 존재하고 있음을 의미한다. 앞에서 언급하였듯이 IPv6 호스트들은 1홉 내에 존재한다고 믿는 노드들에게 패킷을 전송할 경우 ND 메커니즘(ARP)을 수행하여 라우터 없이 패킷을 직접적으로 전달하려고 시도하기 때문에 이를 악용한 공격이 가능할 수 있다.

5) 네트워크 프리픽스 위장 공격

일반적으로 자동 주소 설정 메커니즘을 사용하는 호스트들은 라우터에서 주기적으로 전송하는 RA 메시지에 포함된 네트워크 프리픽스와 네트워크 인터페이스 카드 ID를 이용하여 글로벌 IPv6 주소를 생성한다. RA 메시지를 이용한 자동 주소 설정 메커니즘은 공격 호스트가 네트워크 프리픽스를 위장한 패킷을 노드들에게 전송하여 유효하지 않은 IPv6 주소를 생성하도록 유도하는 데 악용할 수 있다.

6) 파라미터 위장 공격

라우터에 의해서 주기적으로 전송되는 RA 메시지 내에는 해당 네트워크에 속한 호스트들이 자동 주소 설정 메커니즘을 이용하여 IPv6 주소를 생성해야 하는지를 결정하는 것과 같이 통신을 위해 필요한 여러 값을 설정하는 데 필요한 파라미터들을 포함하고 있다. 다른 RA 메시지 위장 공격들과 마찬가지로 이 파라미터들 역시 공격 호스트의 의도에 따라 다른 값들로 변경될 수 있으며 이는 해당 RA 메시지를 수신하는 네트워크 내의 모든 호스트들에게 영향을 미칠 수 있다.

## 4. IPv6 확장 헤더 관련 보안 고려사항

### 가. 라우팅 확장 헤더 관련 보안 문제

IPv6 라우팅 확장 헤더의 라우팅 타입이 0으로 설정되어 있을 경우, 이는 IPv4의 loose source routing 옵션과 동일하게 동작한다. 패킷이 목적지까지 도달하기 위해 거치는 노드들의 라우팅 경로를 임의로 설정할 수 있기 때문에 방화벽 등의 보안 정책을 우회하는 데 다음과 같은 방식으로 악용될 수 있다.

1) 트래픽 필터링 정책 우회 가능성

지정된 노드에서 라우팅 확장 헤더를 처리할 때마다 패킷의 목적지 주소는 다음에 경유할 노드의 주소로 계속 바뀌기 때문에 방화벽 같은 보안 장비가 목적지 IPv6 주소를 기반으로 트래픽 필터링 정책을 설정한 경우 공격자는 라우팅 헤더를 이용하여 이를 우회할 수 있다.

2) 라우팅 헤더를 이용한 추적 우회 가능성

악의적인 사용자는 공격 패킷의 소스 주소를 임의의 주소로 위장하고 라우팅 헤더를 이용하여 해당 패킷이 최종 목적지에 도달하기 전 여러 노드들을 거치도록 함으로써 공격 수행 후 추적을 어렵게 만들 수 있다.

3) ICMP Traceback 회피 가능성

ICMP traceback은 패킷이 전달되는 도중 경유하는 모든 라우터들이 목적지 호스트로 ICMP traceback 메시지를 전달하도록 함으로써 패킷의 소스 주소가 위장되어 설정되었다 하더라도 추후 경유 라우터의 위치를 추적하여 공격 호스트의 위치를 검출해 낼 수 있도록 지원하는 메커니즘이다. 그러나, 라우팅 헤더를 악용하여 사용하게 되면 ICMP traceback 메커니즘을 회피할 수 있는 가능성이 존재한다.

### 나. 단편 확장 헤더 관련 보안 문제

1) 패킷 필터링 정책 우회 공격

IPv6에서는 IP 헤더와 상위 계층 프로토콜 헤더 사이에 여러 확장 헤더가 존재할 수 있기 때문에 최소 단편화된 패킷 크기가 정의되어 있다 하더라도 공격자가 그 크기에 해당하는 확장 헤더를 생성하여 임의로 fragmentable 부분에 삽입하면 TCP와 같은 상위 계층 헤더가 두번째 패킷 이상의 위치에 존재

할 가능성이 있다.

2) Fragment Overlapping 공격

RFC2460 (IPv6 Specification)에서는 단편화된 패킷을 재조합하는 과정에서 나타날 수 있는 fragment offset의 overlapping 문제와 관련하여 어떠한 해결 방안도 제시하지 않고 있기 때문에 IPv4와 마찬가지로 fragment offset overlapping 공격이 가능할 수 있다[6]. 즉, 악의적인 사용자는 공격을 위해 두 개의 단편화된 패킷을 생성한다. 첫번째 단편화된 패킷은 허용된 포트 번호를 포함하기 때문에 방화벽을 통과할 수 있다. 첫번째 단편화된 패킷이 통과하면 이후 같은 fragment ID를 갖는 패킷들은 모두 통과할 수 있도록 허용된다. 이 두 개의 단편화된 패킷이 목적지 노드에 도달하여 재조합되면 첫번째 단편화된 패킷에 저장된 포트번호는 두번째 단편화된 패킷에서 지정한 포트 번호로 겹쳐써지게 된다. 따라서 공격자는 해당 패킷이 겹쳐써진 포트 번호의 응용 프로그램에 접근할 수 없도록 사전에 설정되어졌다 하더라도 방화벽을 우회하여 정상적으로 해당 서비스를 이용할 수 있다.

3) Fragmentation 헤더를 이용한 서비스거부공격

패킷 단편화는 패킷 필터링이나 IDS를 우회하는데 이용될 수 있을 뿐만 아니라 서비스거부공격에도 이용될 수 있다. 즉, RFC2460 IPv6 Specification에 규정된 길이 이상으로 큰 IPv6 패킷을 여러 개의 단편화된 패킷으로 나누어 전송함으로써 공격 목표가 되는 시스템이 해당 패킷을 정상적으로 처리하지 못하도록 서비스거부공격을 유발할 수 있다. 두번째 단편화된 패킷의 옵셋(offset)을 조작하여 해당 패킷들을 재조합하는 과정에서 수신 버퍼를 오버플로시킬 수 있으며 이는 목표 시스템이 정지되거나 재부팅하도록 유발할 수 있다.

다. 확장 헤더 처리 관련 보안 문제

확장 헤더 처리와 관련하여 RFC2460에 명시된 다음과 같은 사항들은 방화벽과 같이 패킷 전달 경로 중간에 놓이는 보안 장비들의 패킷 내용 검사를 수행하는 데 있어 문제가 될 수 있는 소지를 제공한다. RFC2460에서는 hop-by-hop 옵션 헤더를 제외한 모든 확장 헤더들을 중간 노드에서 처리할 수 없도록 명시하고 있다. 또한 목적지 노드에 도착하기 전 패킷을 미리 처리하거나, 이전 헤더를 처리하기 전 임의 헤더의 내용을 살펴보는 행위 또한 허가할 수 없음을 명시하고 있다. 따라서 방화벽 같은 보안장비가 패킷 헤더 검사를 수행하는 것은 RFC에 위배되는 행위일 수 있다.

## 5. 모바일 IPv6 관련 보안 고려사항

가. 라우팅 헤더 관련 보안 문제

앞에서 언급하였듯이 모바일 IPv6에서는 이동 노드의 CoA가 홈 에이전트와 상대 노드에 등록된 후에는 라우팅 헤더를 이용하여 이동 노드와 상대 노드의 통신은 홈 에이전트를 경유하지 않고 직접 이루어질 수 있다. 따라서 모바일 IPv6에서는 라우터뿐만 아니라 모든 노드가 라우팅 헤더를 처리할 수 있도록 요구하고 있다. 그러나 라우팅 헤더는 소스 라우팅 기능을 구현하는 데도 사용될 수 있기 때문에 여러 보안 공격에 악용될 수도 있으며 이를 해결하기 위한 다양한 보안 정책이 고려되어져야 한다.

나. HAO 관련 보안 문제

RFC3775 Mobile IPv6에서는 새로운 라우팅 헤더 형식 2를 정의함으로써 라우팅 헤더가 소스 라우팅을 위해서 사용되는 경우(라우팅 형식 0)와 노드의 이동성을 지원하기 위해서 사용되는 경우를 구분할 수 있도록 하였다[7]. 따라서 보안 장비들은 라우팅 헤더가 소스 라우팅에 악용되는 것을 방지하기 위해서 라우팅 헤더 형식에 따른 필터링 정책을 수행할 수도 있다. 그러나 HAO의 경우 모든 노드에서 반드시 처리되도록 명시되어 있기 때문에 IPv6 노드들은 이를 이용한 여러 공격에 노출될 수 있다. 이

러한 방법으로는 소스 주소 위장 공격이 있을 수 있다. 라우터나 방화벽과 같은 시스템에서는 패킷의 소스 주소가 위장되는 것을 방지하기 위해서 인그레스 필터링과 같은 보안 정책을 유지할 수 있다. 그러나 HAO를 사용하면 소스 주소를 위장한 패킷이 이러한 필터링 정책을 우회하는 것이 가능하다.

다. 바인딩 갱신 관련 보안 문제

모바일 IPv6와 관련한 보안 문제의 근본 원인은 노드의 이동성에 있다. 즉, 특정 이동 노드의 주소가 자주 변할 수 있다는 점이다. 이를 이용하여 해당 노드의 주소를 다르게 알려줌으로써 해당 노드로의 패킷이 다른 호스트로 전달되게 할 수도 있고, 그 노드를 서비스 거부 상태에 이르게 할 수도 있다. 바인딩 갱신에 있어서 발생할 수 있는 보안 문제를 경우별로 살펴보면 다음과 같다. 예를 들면, 공격자가 바인딩 갱신 메시지를 위조하여 홈 에이전트에게 전송하는 경우, 공격자는 어떤 이동 노드에 대해 현재 위치한 곳과 다른 곳에 위치해 있다는 정보를 전송할 수 있다. 만약 홈 에이전트가 이 정보를 받아들인다면 이동 노드는 패킷을 받지 못하는 반면 다른 노드가 원하지 않는 패킷을 수신할 수도 있다. 공격자가 바인딩 갱신 메시지를 위조하여 CN에게 전송하는 경우, 자신의 HA를 victim의 HA로 설정하여 거짓 정보를 알릴 수 있다. 만약 CN이 해당 정보를 받아들인다면 CN에서 victim으로 전송하고자 하는 모든 패킷은 공격 노드를 거치게 되므로 가용성과 기밀성 모두를 위협할 수 있다. 악의적인 이동 노드가 자신의 CoA를 거짓으로 알리는 경우, CN이 해당 이동 노드로 보내는 패킷은 모두 거짓 CoA로 전송되기 때문에 DoS 공격이 가능하다. 특히 다수의 CN으로 victim의 CoA를 갖는 바인딩 갱신 메시지를 전송하면 일종의 DDoS 공격이 가능할 수도 있다. 공격자가 CN으로 의미 없는 바인딩 갱신 메시지를 한 번에 많이 전송할 경우, CN의 자원을 고갈시켜 정상적인 패킷들을 처리할 수 없게 만들 수 있다(DoS 공격). 공격자는 오래된 바인딩 갱신 메시지를 재전송할 수 있다. 만약 이 메시지가 받아들여진다면 현재 이동 노드의 위치로 전달되어야 할 패킷들이 이동 노드의 예전 위치로 전달될 수 있다.

# Ⅳ. IPv6 네트워크 공격기술 및 공격 툴

## 1. IPv4 네트워크 환경과 유사한 공격기술

IPv6 네트워크는 IPv4 네트워크에서 발견되는 대부분의 특성을 유지하기 때문에 IPv4 네트워크에서 발생할 수 있는 보안 취약성 문제들은 상당부분 IPv6 네트워크에서도 나타날 가능성이 존재한다. 이러한 문제로는, 전송 계층 프로토콜의 취약성을 이용한 공격과 ICMPv4 브로드캐스트 또는 ICMPv6 멀티캐스트 취약성을 이용한 공격이 있다. 전송 계층 프로토콜의 취약성을 이용한 공격은, IPv6는 IPv4와 동일한 네트워크 계층의 프로토콜이기 때문에 TCP SYN flooding, TCP ISN, UDP flooding 공격과 같이 전송 계층 프로토콜의 취약성으로 인한 공격은 여전히 발생할 가능성이 존재한다. 현재 IPv6 호스트를 스캐닝한 후 flooding 공격을 시도하는 imps6-tools와 같은 공격 툴들이 이미 등장하기 시작하였다. ICMPv4 브로드캐스트 또는 ICMPv6 멀티캐스트 취약성을 이용한 공격은, IPv4 네트워크에서 발생 가능한 기존의 공격 기법들은 IPv6 환경에 맞는 새로운 형태로 변형될 가능성이 존재한다. 예를 들어 IPv6에서는 브로드캐스팅이 존재하지 않기 때문에 IPv4의 스머프 공격을 그대로 적용할 수 없으나, 멀티캐스팅이 IPv4의 브로드캐스팅과 유사한 특징을 갖기 때문에 멀티캐스팅 메시지 증폭을 이용한 공격으로 변형될 수 있다.

## 2. IPv4/IPv6 네트워크간 전환기술을 이용한 공격기술

현재 IPv6가 IPv4를 완전히 대체하기까지는 상당히 많은 기간이 소요될 것으로 예측되고 있기 때문에 다음과 같은 다양한 전환 기술들을 사용하여

IPv4 네트워크와 IPv6 네트워크가 장기간 공존하는 형태를 이룰 것으로 예상된다[8]. IPv4/IPv6 네트워크 전환 기술에는 듀얼 스택(dual stack), IPv6-to-IPv4 터널링 기술, 변환(translation) 메커니즘 등이 있다. 따라서 IPv6 도입 초기에는 이러한 전환 기술들을 악용한 공격이 발생할 가능성이 존재하며, 최근 이 기술들을 악용하는 불법 IPv6-to-IPv4 터널링 생성 툴, IPv6-to-IPv4 터널링 기반 서비스거부공격 툴들이 등장하기 시작했다[9]. 불법 IPv6-to-IPv4 터널링 생성 툴의 경우, 일반 IPv4 호스트는 IPv6 호스트에 접근할 수 없으나 악의적인 IPv4 호스트가 IPv6 호스트에 접근할 수 있도록 불법적인 터널링을 생성해주는 Relay6, 6tunnel, nt6tunnel, asybo와 같은 툴들이 존재한다. 이러한 툴들은 IPv6 호스트를 직접적으로 공격하지는 않지만 악의적인 사용자로 하여금 IPv6 호스트에 접근하도록 하여 backdoor나 trojan과 같은 불법 코드를 설치할 수 있는 빌미를 제공할 수 있다. IPv6-to-IPv4 터널링 기반 서비스거부공격 툴은 6To4DDoS, 6tunneldos와 같은 툴들은 터널링 기술을 사용하여 임의의 IPv6 호스트와 IPv4 호스트에 대한 서비스 거부공격을 수행할 수 있다. 또한, 6to4 터널링에 적용될 수 있는 공격 형태는 공격 대상 호스트(victim)가 다른 호스트들과 통신하는 것을 막기 위한 서비스거부공격, 다른 호스트들로 전송되는 패킷을 공격 대상 호스트에게 리다이렉션 함으로써 서비스거부공격을 유발하는 reflection 공격, 악의적인 호스트가 불법적으로 IPv6 서비스를 획득하기 위한 service theft 공격 등으로 분류할 수 있다.

## 3. 순수 IPv6 네트워크에서의 공격기술

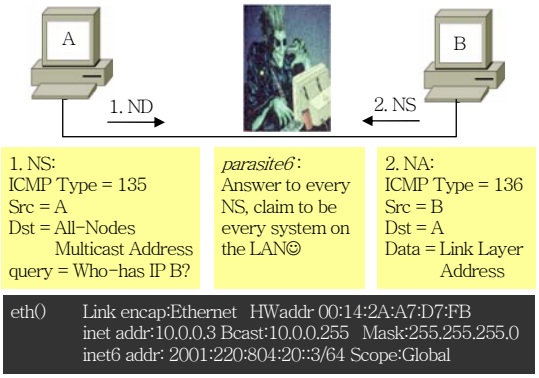
IPv6에 새롭게 추가된 필드나 기능들을 악용하여 이전의 IPv4 네트워크에서는 발견할 수 없었던 새로운 형태의 공격이 발생할 가능성이 존재한다. 예를 들어 IPv6의 광범위한 IP 주소 공간과 자동 주소 설정 기능을 악용한 서비스거부공격은 IPv4 보다 대응을 더 어렵게 할 수 있다. 이러한 공격형태는 IP 헤더의 flow label 필드를 이용한 서비스거부공격, 주소 자동 설정(auto-configuration) 기능을 악용, NS/NA 메시지를 악용한 공격 등이 있을 수 있다. IP 헤더의 flow label 필드를 이용한 서비스거부공격의 가능성으로는, IPv6에서는 IP 주소와 flow label 필드를 이용하여 특정 네트워크 트래픽 flow를 정의하고, 그 flow에 따라 서비스를 차등 제공할 수 있는 메커니즘 제공하고 있다[10]. 주소 자동 설정 기능을 악용한 공격 가능성으로는, IPv6에서는 RA 메시지를 이용하여 전송되는 네트워크 프리픽스와 노드의 인터페이스 주소를 결합하여 쉽게 IP 주소를 생성할 수 있도록 해주는 자동 주소 설정 기능 제공하고 있는데, 이러한 특징으로 악용될 가능성이 있다. 예를 들면, 공격 후 사용하던 NIC을 교체하여 다른 IP 주소를 할당 받게 되는 것만으로도 공격자 추적을 어렵게 하여 공격자의 신분 위장에 악용될 수 있고, 올바르지 않은 네트워크 프리픽스 전송을 통한 서비스거부공격의 가능성이 있다. 또한, 자동 주소 설정과 DAD를 악용한 서비스거부공격의 가능성이 있고, 파라미터 위장 공격에 악용될 소지가 있다. IP 주소를 통해 사용자의 의사와 상관없이 사용중인 하드웨어 정보가 노출될 가능성이 있다. NS/NA 메시지를 악용한 공격의 가능성은, NS/NA 메시지는 이웃 노드의 링크 계층 주소를 결정하는데 사용된다[11]. 그러나, 공격자가 악의적인 목적으로 NS 메시지 내에 위장된 source link-layer address 옵션 값을 설정하거나 NA 메시지 내에 위장된 target link-layer address 옵션을 설정하여 전송하면 이를 수신한 호스트는 잘못된 네이버 캐시 내역을 생성하게 되기 때문에 이후 전달되는 패킷은 의도하지 않은 다른 호스트의 인터페이스로 전달될 가능성이 존재한다.

## 4. IPv6 환경에서의 네트워크 공격 도구

### 가. THC 도구를 이용하는 IPv6 이상 트래픽

THC[12]라는 곳에서 최근에 IPv6상에서 다양한 공격 트래픽을 생성할 수 있는 도구를 발표하였다. 이를 활용한 주요 IPv6 공격은 다음과 같다.

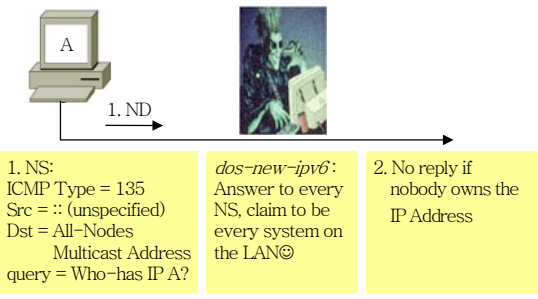
• Parasite6: (그림 2)와 같이 ICMPv6 neighbor spoof를 하여 IPv6 트래픽을 가로채는 공격이다. A라는 노드가 B 노드에게 데이터를 전송하기 위해서 B의 MAC을 알고 싶을 때 멀티캐스트 주소(ff02::1)로 ICMPv6 ND(메시지 타입: NS) 메시지를 보내고, 노드 B는 응답으로 NA 메시지를 A에게 보내게 된다. 그러나 이 메시지를 가로채서 NA 메시지에 부정확한 MAC 주소를 삽입하여 보내면 A는 B에게 데이터를 전송할 수 없게 된다.




(그림 2) THC 도구: parasite6

Parasite 공격과정을 보면 어떤 노드에서 ICMPv6 메시지가 발생하면 공격자가 감시하고 있다가 패킷을 가로채어 MAC 주소를 변경하여 다시 네트워크에 전송하게 된다. 변경된 MAC 주소가 로컬링크에 존재한다면 수정된 ICMP 메시지를 수신하게 되고 IPv6 주소가 맞지 않아 리다이렉트를 하게 된다.

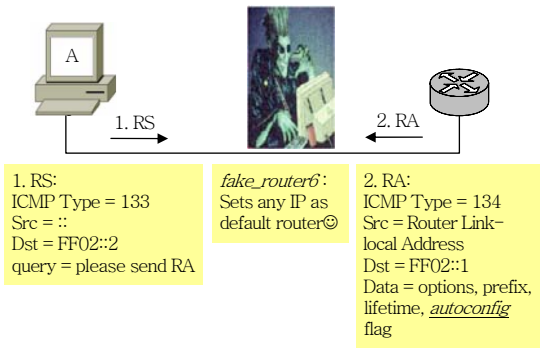
• Dos-new-ipv6: (그림 3)과 같이 새로운 호스트가 랜에 연결될 때, 중복 IP 주소 검사를 방해하여 연결되지 못하도록 하는 공격이다. 특정 노드가 IPv6 네트워크에 연결되면 자동으로 링크로컬 주소를 생성하고 링크에 중복되는 노드가 없는지 ND(메시지 타입: NS)를 멀티캐스트 주소(ff02::1)로 보내어 조사를 하게 된다. 이때 NA 메시지가 일정 시간 동안 오지 않으면 특정 노드는 자신이 생성한 링크로컬 주소를 사용하게 된다. thc-ipv6의 dos-new-ipv6 툴은 DAD를 위한 메시지를 감시하고 있다가 DAD를 위한 메시지가 발생하면 NA 메시지를 응답하여 새로 연결된 노드가 링크로컬 주소를 설정하지 못하도록 방해한다.




(그림 3) THC 도구: dos-new-ipv6

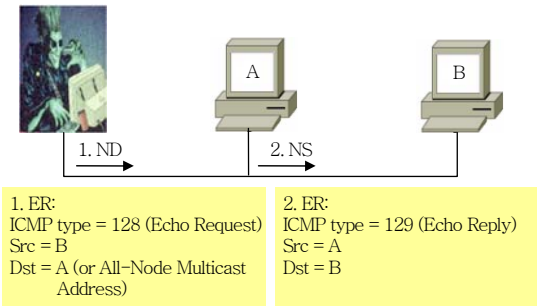
• Redir6: 트래픽을 다른 곳으로 전송하게 하는 공격

• Fake_router6: (그림 4)와 같이 가짜 라우터로 행세하게 하는 공격이다. 라우터는 링크로컬의 모든 노드에게 멀티캐스트 주소(ff02::1)로 주기적으로 라우터임을 알리는 RA ICMPv6 메시지를 보낸다. RA 메시지를 받은 노드들은 라우팅 테이블과 네트워크 프리픽스 정보를 설정하게 된다. 이러한 ICMPv6 메시지를 이용하여 thc-ipv6의 fake_router6 도구는 잘못된 RA 메시지를 발생하여 링크로컬의 모든 노드들의 라우팅을 방해할 수 있다.




(그림 4) THC 도구: fake_router6 공격

• Smurf6: (그림 5)와 같은 IPv6에서의 증폭공격이다. IPv4 네트워크에서 가능했던 공격으로 ICMP echo request 메시지를 이용하여 제 3자




(그림 5) THC 도구: smurf6 공격

가 victim을 공격하는 것으로 IPv6 네트워크에서도 가능하다. 스머프 공격을 ICMP echo request 메시지 대량으로 발생시켜 victim의 시스템의 가용자원 및 네트워크 대역폭을 점유하도록 하여 victim이 네트워크 서비스를 못하도록 한다. thc-ipv6의 smurf6 도구는 ICMP6를 이용하여 스머프 공격을 할 수 있다.

- Fake_mipv6: MIPv6에서 핸드오버 메시지인 BU를 가로챌 수 있는 공격

### 나. IPv6 프로토콜을 이용하는 은닉 채널 통신 트래픽

은닉 채널(covert channel)이라고 하는 것은 TCP/IP 프로토콜의 필드들 중 사용이 안되는 필드들을 이용하여 통신에 활용하는 기법이다[13],[14]. 이를 이용하여 IRC 채팅에 활용하여 공격 트래픽을 유발한다고 알려져 있다.

- Hop limit 필드를 조작하는 기법: hop limit 필드의 값을 두 가지 종류로 구분하여 전송하여 0 또는 1비트를 나타내도록 한다.
- Hop-by-hop 옵션: 점보그램의 길이를 조작하여 숨겨진 정보를 전송하는 데 사용한다.
- DO: 현재는 MIPv6에서 BU만 정의되어 있는데, 이것을 제외한 다른 필드들을 이용하여 통신을 하도록 한다[15]. 이는 2003년도에 Thomas Graf에 의해서 알려진 것으로 http://trash.net/~reeler/j6p.tar.bz2에 공개되어 있다. 이 공격은 DO에서 option type의 상위 2비트의 값이 00이면 이 옵션을 건너뛰어 헤더 처리를 계속하도록 하게 한다. 01이면 패킷을 버리게 된다. 따라서, 00으로 설정하여 채팅 메시지를 전송하게 한다.

IPv6-over-IPv4 터널링 트래픽: IPv4에서 IPv6로 전환을 하는 동안에는 IPv6-over-IPv4 터널링이 많이 사용될 것으로 전망된다. SIT, 6to4, Teredo[16] 등의 터널링 기법이 사용되고 있다. 특히, 6to4 터널링 기법은 동적으로 터널을 생성할 수 있기 때문에 보안의 취약점으로 작용할 수 있다. 하지만, 6to4 터널링 기법은 2002::/16의 프리픽스를 사용하고 있고, 터널링은 41번 프로토콜 값을 이용하고 있기 때문에 쉽게 탐지될 수 있다. 하지만, UDP를 기반으로 하는 Teredo와 같은 터널링 기법은 탐지되기 어렵다.

## V. IPv6 네트워크 공격 및 침해요소에 대한 대응 방안

여기서는 IPv6 환경에서의 네트워크 공격 및 침해요소에 대한 대응 방안으로 크게 IPv6 침입탐지 및 차단 기술 관점에서의 대응과 방화벽, 침입탐지/차단 시스템이 제공해야 할 기능적 특성에 대해서 설명한다.

### 1. IPv6 침입탐지 및 차단기술 관점에서의 대응 방안

방화벽을 우회할 수 있는 ESP 트래픽 대응 방안으로는 신뢰성이 입증된 특정 호스트를 제외한 나머지 호스트들에서 전송되는 ESP 트래픽은 모두 차단, 방화벽을 신뢰성 있는 중간 노드로 설정하여 종단 노드 간에 수행되는 모든 IPsec 과정이 방화벽을 경유하여 이루어지도록 하는 보안정책 적용, 호스트 기반의 방화벽(distributed firewall or personal firewall)과 연계하여 복호화된 후 IPsec 패킷의 내용 검사 등이 있다. RFC3041[17]의 프라이버시 확

장기법 및 DAD에 대한 대응 방안으로는, 방화벽의 접근 제어 리스트에 프라이버시 확장기법에 의해 변경되는 IP가 반영될 수 있도록 지원, DAD가 서비스 거부공격에 악용될 수 있으므로 이 기법에 관여되는 모든 패킷을 IPsec의 AH 헤더를 이용한 인증 후 사용할 수 있도록 하거나 DAD 패킷 모니터링 기능을 방화벽 및 침입탐지/차단 시스템에서 지원 등이 있다. ND 메커니즘 및 주소 자동 설정 관련 대응 방안으로는, ND 메커니즘과 주소 자동 설정 메커니즘은 IPv6 프로토콜이 정상적으로 동작하기 위해 반드시 필요한 매우 중요한 구성 요소임에도 불구하고 여러 보안 공격에 악용될 수 있기 때문에 해당 메커니즘을 수행하는 데 필요한 메시지의 신뢰성을 보장하는 방안이 요구된다. 따라서, 이 메커니즘을 안전하게 실행하기 위해 SEND를 사용하거나 방화벽 및 침입탐지/차단 시스템에서 해당 메커니즘을 수행하는 데 필요한 메시지에 대한 모니터링 및 관리를 위한 기능 지원이 필요하다. IPv6 확장 헤더 관련 대응 방안으로는, 라우팅 확장 헤더를 이용하여 트래픽 필터링 정책 우회 및 추적 우회 가능성을 차단하기 위해서 경유경로상에 존재하는 호스트도 필터링 정책에서 처리할 수 있도록 지원 필요, 패킷 필터링 정책 우회, fragment overlapping, 서비스거부공격에 사용될 가능성을 차단하기 위해서 IPv6 확장 헤더가 포함된 모든 패킷의 용도를 검사할 수 있는 패킷 필터링, 침입탐지/차단 규칙에 대한 지원이 필요하다.

### 2. 방화벽, 침입탐지/차단 시스템이 제공해야 할 기능적 특징

기능적 특성으로는, 방화벽에서는 어떠한 확장 헤더 등이 통과하고 처리되어야 하는지 처리할 수 있도록 지원, 보더 라우터에서는 내부망에서 사용될 IPv6 주소 필터링 규칙 정의 지원, ICMPv4 및 ICMPv6 패킷(Type 2, 4, 130-136)에 대한 필터링 지원, 1280 옥텟 이하의 모든 프래그먼트 부분은 폐기, IPv6 지원 인그레스 필터링, 터널링 및 IPv4/IPv6 전환 메커니즘에 사용되는 프로토콜 및 포트 번호 처리 지원이 필요하다. 또한, 이와 더불어서 보안 강화가 필요한 중요한 시스템의 경우는 static ND 엔트리를 정의하여 사용하거나, BGP, IS-IS 등 라우팅 프로토콜상에 인증 및 보안 메커니즘 사용, OSFPv4, RIPng 등에 IPsec 사용, 6to4와 같은 동적 터널링보다는 정적인 터널링을 사용하는 방법이 필요하다[18].

## Ⅵ. 맺음말

IPv6 환경에서는 기존의 IPv4 환경과는 다르게 IPv6 프로토콜에 새로이 등장하는 특징으로 인한 취약점이 존재하여 지금까지 살펴본 위협요소와 보안 고려사항을 수용한 대응 방안이 필요하다. 이를 위해 IPv6로 전환시 보안 위협, IPv6 침입탐지 및 차단을 위한 보안 고려사항, IPv6 네트워크에서의 공격기술 및 공격 툴, IPv6 네트워크 공격 및 침해요소에 대한 대응 방안 등에 대해서 설명하였다. 향후 몇 년 이내로 IPv6 표준화가 완성되고, 상용제품이 활발하게 등장하기 시작하면 본격적인 IPv6 도입이 가시화 될 것으로 예측된다. 이러한 상황에서 본 고에서 살펴본 바와 같은 IPv6 네트워크를 안전하게 운용할 수 있는 네트워크 보안기술 및 독자적인 보안 시스템들의 개발은 필수적이며, IPv6 환경에서 발생 가능한 네트워크 공격방법과 대응 방안에 대한 핵심기술의 확보가 반드시 필요하다고 할 수 있다.

## 약 어 정 리

| | |
|---|---|
| ACL | Access Control List |
| BcN | Broadband convergence Network |
| BU | Binding Update |
| CN | Correspondent Node |
| CoA | Care-of Address |
| DAD | Duplicate Address Detection |
| DO | Destination Option |
| ESP | Encapsulating Security Payload |
| HA | Home Address |

| | |
|---|---|
| HAO | Home Address Option |
| IDL | Interface Definition Language |
| IDS | Intrusion Detection System |
| IKE | Internet Key Exchange |
| IPS | Intrusion Prevention System |
| ISN | Initial Sequence Number |
| NA | Neighbor Advertisement |
| ND | Neighbor Discovery |
| NIDS | Network-based IDS |
| NS | Neighbor Solicitation |
| NUD | Neighbor Unreachability Detection |
| RA | Router Advertisement |
| RMON | Remote Monitoring |
| RS | Router Solicitation |
| SEND | Securing Neighbor Discovery |
| SNMP | Simple Network Management Protocol |
| THC | The Hacker's Choice |

## 참 고 문 헌


[1] 2005 IPv6 동향, 정보통신부/한국전산원, 2005.

[2] Cisco NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/netflct/tech/napps_ipfix-harter.html.

[3] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC2462, Dec. 1998.

[4] P. Nikander, J. Kempf, and E. Nordmark, "RFC3756: IPv6 Neighbor Discovery (ND) Trust Models and Threats," IETF, May 2004.

[5] T. Narten, E. NOrdmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," RFC2461, Dec. 1998.

[6] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC2460, Dec. 1998.

[7] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC3775, June 2004.

[8] R. Gilligan and E. Nordmark, "RFC2893: Transition Mechanisms for IPv6 Hosts and Routers," IETF, Aug. 2000.

[9] Michael H. Warfield, "Security Implications of IPv6," Internet Security Systems, 2003.

[10] J. Rajahalme, A. Conta, B. Carpenter, and S. Deering, "RFC3697: IPv6 Flow Label Specification," IETF, Mar. 2004.

[11] T. Narten, E. Normark, and W. Simpson, "RFC2461: Neighbor Discovery for IP Version 6," IETF, Dec. 1998.

[12] The Hackers' Choice Attack Tool, http://thc.segfault.net/

[13] Norka B. Lucena, Grzegorz Lewandowski, and Steve J. Chapin, "Covert Channels in IPv6," Workshop on Privacy Enhancing Technologies, 2005.

[14] D. Llamas, C. Allison, and A. Miller, "Covert Channels in Internet Protocols: A Survey," Workshop on Privacy Enhancing Technologies, 2005.

[15] T. Graf, "Messaging over IPv6 Destination Options," The Swiss Unix User Group, Switzerland, http://gray-world.net/papers/messip6.txt, 2003.

[16] C. Huiteman, "Teredo: Tunneling IPv6 over UDP through NATs," RFC4380, Feb. 2006.

[17] T. Narten and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," RFC 3041, Jan. 2001.

[18] 신명기, 김형준, "IPv6 전환 환경에서의 보안 기술 분석," 전자통신동향분석, 제 21권 제 5호, 2006, pp.163-170.