KISA 안내 · 해설 제2010-25호

IPv6 보안 기술 안내서

2010. 2

KISA
한국인터넷진흥원

주 의 사 항

본 안내서의 사용에는 제한이 없으나 다음과 같은 사항에 주의하여야 합니다.

- 문서 내에 언급된 상표, 제품명 등에 대한 권리는 각 상표 또는 제품을 소유한 해당 기업에 있으며, 설명을 위하여 특정 회사 제품명 또는 화면이 표시된 경우 IPv6 보안기술에 대한 이해를 높이고자 하는 목적 외에 어떠한 다른 목적도 없으며 그렇게 이용되어서도 안 됩니다.

- 문서 내에 기술된 내용들은 일반 사용자, 기업 등에 있을 수 있는 고유환경을 고려하지 않았습니다. 또한 현재 시점에서 작성된 것이므로 이후 변경되는 사항에 의하여 발생하는 피해에 대하여 이 해설서의 발행기관은 책임을 지지 않습니다.

※ 본 안내서의 내용 중 오류가 발견되었거나 내용에 대한 의견이 있을 때에는 한국인터넷진흥원으로 해당 내용을 보내주시기 바랍니다.

KISA 안내 · 해설 제2010-25호

IPv6 보안 기술 안내서

2010. 2

KISA
한국인터넷진흥원

제·개정 이력

순번	제·개정일	변경내용	발간팀	연락처
1	2010.1.1	제정	융합보호R&D팀	405-6311
2				
3				
4				

정보화가 급속하게 진전됨에 따라 정보기기간의 통신이 중요한 요소로 부상하고 있으며, 유선 및 무선 네트워크 환경에서의 ALL-IP화가 진행되고 있습니다. 또한 IP 통신기능을 갖는 가전기기, 휴대단말 기기의 수요가 늘어남에 따라 IPv6 인프라 확충에 대한 요구 또한 증가하고 있습니다.

국내에서는 IPv6의 조기 정착 및 활성화를 위하여 정부주도의 IPv6 시범사업을 추진하고 있으며, 전 세계적으로 IPv6 주소를 네번째로 많이 가지고 있는 우리나라에서는 앞으로 수년 내에 많은 IPv6 관련 서비스가 상용화될 것으로 예상됩니다.

이와 함께 IPv6의 보급 확산을 위해서는 인터넷을 통한 다양한 침입과 침해로부터 정보통신 단말과 네트워크 장비들을 보호하고, 네트워크를 통하여 전송되는 정보를 보호하면서 나아가 정보통신망 자체까지 보호할 수 있는 보안 기술이 필수적으로 요구됩니다. 이러한 기술은 기존 IPv4에서 이루어지던 보안 기술과 더불어 IPv6에서 새로이 제기되는 보안 요구를 충족할 수 있어야 합니다.

한국인터넷진흥원에서는 IPv6 네트워크 환경에서의 다양한 공격에 대한 피해를 예방하고 IPv6 보안에 대한 이해를 증진시키기 위하여 IPv6 네트워크 운영자와 IPv6기반 솔루션 개발자를 대상으로 IPv6 보안 기술 안내서를 발간하게 되었습니다.

본 보안기술 안내서는 ISP, 일반기업 등 IPv6 네트워크의 도입 계획이 있거나 현재 운영하고 있는 기관에서 안전한 IPv6 네트워크 운영 및 관리를 위한 참고 자료로 활용될 수 있으리라 생각됩니다. 또한, 보안 솔루션 개발 업체에서는 기술 개발 시 고려해야 할 보안취약성에 대해 참고할 수 있을 것입니다. 본 IPv6 보안 기술 안내서가 현장에 계신 많은 분들에게 도움이 될 수 있기를 바라며 본 기술 안내서의 작업에 의견을 주신 분들께 깊이 감사드립니다.

2010년 2월

한국인터넷진흥원장 김희정

본 안내서는 안전한 IPv6 네트워크 환경 구축 및 운영을 위해 필요한 보안 취약성 및 대응방안에 대한 정보를 제공한다. IPv6 표준에 명시된 기능들에 대한 새로운 보안 취약성과 대응방안을 설명하며, IPv4와 IPv6간의 전환에 따른 보안취약성과 대응방안도 함께 제공한다. 그러나, IPv6 환경에서의 스위치에 대한 공격, 바이러스, 웜 등 데이터링크 계층 및 응용 계층에 대한 보안 취약성과 대응방안들은 다루지 않는다.

IPv6 네트워크 환경에서의 보안취약성 및 대응방안을 설명하기 위한 본 안내서는 총 5장으로 구성되어 있다. 각 장의 구성과 내용은 다음과 같다.

구성 및 활용

1장에서는 IPv6의 개념 및 활용방안을 설명한다. IPv6의 등장 배경 및 IPv4와의 차이점 비교를 통하여 IPv6의 특징을 파악할 수 있다. 그리고 IPv6의 도입 내용 및 정보 보호 제품에 대한 현황 분석을 통하여 IPv6 보안 제품 개발에 대한 전망을 설명한다.

2장에서는 IPv6 프로토콜의 새로운 기능에 대한 보안 취약성에 대하여 유선망과 이동망으로 구분하여 분석하고 각각에 대한 대응방안을 설명한다.

3장에서는 IPv4에서 IPv6로의 전환(transition)기술과 관련된 듀얼 스택, 터널링 그리고 변환(translation) 기술로 구분하여 설명하고 각 기술별 보안 취약성 및 대응방안을 설명한다.

4장에서는 IPv4 및 IPv6 네트워크 환경에서 공통적으로 나타날 수 있는 보안 공격들에 대하여 설명하고 각각의 대응방안을 설명하고 5장에서는 결론을 맺는다.

본 안내서는 유선환경 및 이동환경에서 IPv6를 도입, 구축, 운영하고자 하는 경우에 활용될 수 있으며, IPv6 기반의 보안 응용을 개발하는 경우에도 참고자료로 활용 가능하다. 더불어 IPv4 네트워크 환경에서의 정보 보호 관련 가이드와 함께 활용할 것을 권장한다.

목차

IPv6 Security

Contents

제 3 장 IPv4/IPv6 전환기술의 보안취약성 및 대응방안

제 4 장 IPv4/IPv6 공통 보안취약성 및 대응방안

Contents

목차

IPv6 Security

표목차

그림목차

Contents

목차

IPv6 Security

제 1 장 IPv6 개요

제 1 절 IPv6 등장 배경 및 동향

1. 등장 배경

현재 사용되고 있는 인터넷 프로토콜인 IPv4(Internet Protocol Version 4)는 컴퓨터와 인터넷 등 네트워크의 광범위한 사용을 예측하지 못하던 시대에 등장하였다.

IPv4가 도입되던 시기에는 컴퓨터를 활용하는 사용자가 뛰어난 기술적 능력을 가진 소수의 학자와 기술자로 한정되어 있어, 해당 사용자가 실수로 다른 사람의 장비 · 자원 · 업무를 침해하지 않는 최소한의 보안 수준으로도 운영이 가능하였다. 그러나 컴퓨터와 네트워크의 사용이 보편화된 현재에는 해킹 · 바이러스를 비롯한 인터넷 침해사고로 인한 피해가 점점 증가하고 있을 뿐 아니라 다가올 유비쿼터스 환경에서는 보안의 중요성이 더욱 강조될 것으로 예상된다.

IPv4는 이론상 43억여개의 인터넷 주소를 지원할 수 있다. 그러나 클래스 단위로 주소를 구분하는 비효율적인 주소체계와 매년 급증하는 인터넷 접속 호스트 수로 인해 인터넷 주소 고갈의 우려가 대두되고 있다. 또한, IPv4에는 QoS 기능이 없어 특화된 서비스의 제공이 어려웠다.

IPv6는 IPSec(Internet Protocol Security)이라는 자체 보안 요소를 탑재하고 주소공간을 대폭적으로 확대한 인터넷 프로토콜로서 IPv4의 문제점을 해결할 수 있을 것으로 기대된다. 또한 플로우 레

이블(Flow Label)을 이용한 패킷별 품질제어 및 주소 자동 설정(Address Auto-configuration) 등의 기능도 추가되어 관리자와 일반 사용자의 편의성도 증대될 것이다. 한편, IPv4/IPv6 전환 시의 보안이 이슈화되는 등 현실적인 문제점과 그에 대한 해결책도 구체적으로 제시되고 있는 추세이다.

정보통신부는 2003년 9월에 'IPv6 보급 촉진계획'을 수립하여 국가 정책으로 채택하고, IPv6 보급 촉진을 통해 차세대인터넷 산업과 신규 서비스를 육성함으로써 인터넷 소비국에서 생산 강국으로 도약하였다.

특히 정부통신부의 IT 성장전략인 IT839전략 안에 IPv6의 첨단 인프라구축을 포함시켜 향후 IPv6로의 전환을 위해 적극적이고 체계적인 노력을 하고 있다. [그림 1-1]은 정부가 추진 중인 로드맵의 유?무선망에 대한 IPv6 적용 계획을 나타낸다.

그림 1-1 유 · 무선망에 대한 IPv6 적용 계획

정부추진 로드맵	2004년	2005년	2006년	2007년	~2010년
	시범망	유선 상용망	무선 상용망		
KT	IPv6 테스트베드 확대 구축 및 검증	IPv6 시험망	BcN 및 광대역통합국가망 IPv6 상용화		ALL-IPv6 인프라 구축
데이콤	IPv6 시범망 구축 VoIP, VoD 등 개발	광대역통합국가망 IPv6 상용화	보라인터넷망 IPv6 상용화		IPv6 Only 구현
하나로텔레콤	IPv6 기능 검증	DcNA 시범서비스망	개별 상용화	확대적용	
SK텔레콤	인프라 장비, 단일 IPv6 개발 추진	백본망/접속망에 대한 IPv6 상용화 기반 구축	부가 / 플랫폼 장비 IPv6 전환 및 상용 서비스		ALL-IPv6 진화
KTF	IPv6 CDMA/WCDMA 시범망 구축	IPv6 IMS/Open API 시범망 구축	IPv6 상용 서비스		ALL-IPv6 상용망 구축
LG텔레콤	CDMA 기반 Mobile IPv6 시험망 구축	CDMA 패킷망 Dual Stack 상용망 구축, 시범 서비스 실시	상용망		서비스 계획

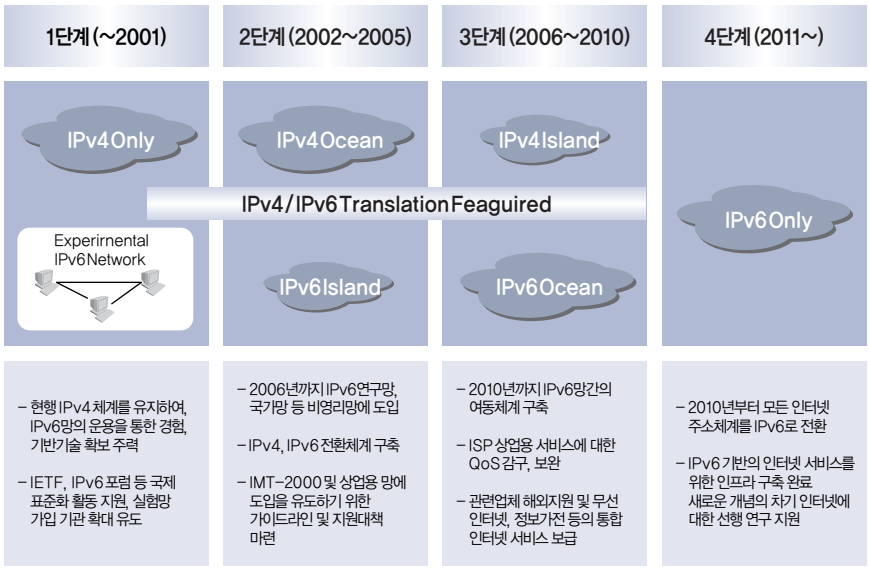
※ 자료출처 : IT839 인프라 전략 협의회 발표자료, 2005. 5

'IPv6 보급 촉진 기본계획'은 2003년 9월 발표된 'IPv6 보급 촉진계획'을 관련기관 및 산업체의 최고책임자로 구성된 'IPv6 전략 협

의회' 를 통해 3차례 협의를 거쳐 최종 확정된 것이다.

IPv6 보급 촉진을 통하여 차세대인터넷 산업과 서비스를 육성함으로써 터넷 소비국에서 생산국으로 도약한다는 추진목표 아래 2004년에 IPv6 시범망을 확대 구축하고 2005년부터 상용서비스를 발굴하여 2010년 이후 All-IPv6 기반의 서비스를 제공할 것을 목표로 하고 있다. [그림 1-2]는 'IPv6 보급 촉진 기본계획' 에 대한 추진계획을 나타낸다.

그림 1-2 'IPv6 보급 촉진 기본 계획' 추진계획



※ 자료출처 : 정보통신부, IPv6 보급 촉진 기본계획

'IPv6 보급 촉진 기본계획' 은 4개의 핵심전략으로 구성되어 있으며 내용은 다음과 같다.

4대 핵심전략

- **국내 환경에 맞는 통신장비와 서비스를 개발하고, 보안성, 이동성, VPN 등 차별적 기능을 선택 개발 유도**
- **BcN, WiBro, 홈네트워크 가전 보급 등 유관사업과 연계 추진**
- **정부, 공공 및 연구분야에 선도적으로 보급하여 초기시장 조성**
- **정부, 학계, 산업체, 연구계 및 사용자와의 협력체계 강화**

'IPv6 보급 촉진 기본계획' 에 따라 국내 IPv6의 조속한 확산을 위해 정보통신부는 2005년 차세대 인터넷주소체계(IPv6) 사업에 많은 예산을 투입하여 관련 장비 개발을 지원하는 한편 정부망을 중심으로 우선 도입키로 확정했다. 2005년 신규 구축되는 전자정부통신망에는 IPv6 장비가 도입되고, 정보통신부 기반망(MIC-Net)의 고도화에 IPv6 장비가 투입되었으며, 국방부 등 정부기관의 IPv6 도입도 적극 확산해 나가고 있다.

2. 필요성

IPv6는 유비쿼터스, BcN(Broadband convergence Network), 홈네트워크 서비스 등을 구축하기 위한 핵심 인프라 기술로서 우리나라를 포함한 세계 각국은 IPv6 도입을 적극적으로 추진하고 있다. [표 1-2]는 각국의 IPv6 활성화 현황 이다.

가. 유비쿼터스 서비스 구축 환경 조성

현재 정보통신 서비스는 유 · 무선 통합망을 기반으로, 다양한 종류의 단말과 장비를 통해서 모든 사물과 콘텐츠에 접근이 가능하며 각종 멀티미디어를 복합적으로 응용할 수 있는 유비쿼터스 서비스를 지향하고 있다. 이러한 유비쿼터스 장비 및 서비스의 제공을 위해 IPv6 도입은 필수적이다.

표 1-1 각국의 IPv6 활성화 계획 현황

국가	추진내용
한국	– IPv6 보급 촉진을 통한 차세대 인터넷 산업 및 서비스 육성 – 2010년 ALL-IPv6 기반 서비스 제공 – 정부, 공공 및 연구분야에 선도적으로 보급하여 초기시장 조성
미국	– 미 국방성은 국방망에 2008년까지 IPv6 도입 – Cisco, MS 등 민간중심으로 연구개발 – IPv6 시험/검증을 위한 대규모 네트워크 실험 프로젝트 시행 – 라우터, 운영체제 등에서 세계시장 석권
일본	– IPv6 장비개발 및 채택에 대한 세금우대정책 시행 – IPv6 Promotion Council을 중심으로 민 · 관 협력 추진
EU	– 연 1,100억원 규모의 IPv6 적용 연구과제 추진 중 – Eurov6를 통한 IPv6 홍보 및 IPv6장비 시험장 구축
중국	– 연구교육망인 CERNET을 통해 IPv6 테스트베드 구축 관련 연구 진행 – 정부주도로 순수 IPv6망 구축사업인 CNGI 프로젝트 진행 – 민간주도의 "IPv6 Council"을 설립하여 IPv6 보급 활동 진행

※ 자료출처 : 한국전산원 「IPv6동향2004」, 2004

나. 홈네트워크 서비스 구축 환경 조성

가정 내 정보가전의 증가 및 가입자망의 전송 속도 향상에 따라 홈네트워크 서비스의 구축이 점점 현실화되고 있다. 이러한 홈네트워크에 연결될 PC, 냉장고, TV 등의 장비는 국가경제를 이끌 신성장 동력으로서 다양한 응용서비스와 연동될 것이다. 향후, 홈네트워크가 활성화될 경우, 사용자가 인터넷을 매개로 정보가전 기기에 접속하고 통제하기 위해 IP주소의 필요성이 급격히 증가할 것이며, 이에 따라 IPv6 도입이 필수적이다.

다. BcN 구축을 위한 ALL-IP 환경 조성

현재 인터넷을 통해 데이터 서비스뿐만 아니라 전화, 방송 등 기존의 정보통신서비스를 전송할 수 있는 기술적 기반은 이미 확보되어있다. 특히, 이동통신망이 현재의 유선 ISP망과 연동되면 대부분의 네트워크가 IP를 수용하게 되면서 인터넷은 명실상부한 정보통신서비스 종합전달망의 위치를 확보하게 될 것이다. 이러한 ALL-IP 시대를 준비하기 위해 현재의 IPv4 체계로는 서비스 수용의 한계가 예상되며 IPv6 도입이 필수적이다.

[표 1-2]은 IPv6 기반 비즈니스 모델의 특징이다.

표 1-2 IPv6 관련 비즈니스 모델의 특징

특징	세부특징
새로운 기술	– 주소공간의 제한이 거의 없음 – built-in 보안(IP Security) 및 향상된 품질제어(QoS)기능 제공 – 이동성 및 주소 자동 설정(Address Auto-configuration) 도입
새로운 서비스	– 쉽고 편리하고 안전한 서비스 – 언제 어디서나 자유로운 통신서비스 – 유 · 무선 통합형 멀티미디어 서비스
새로운 비즈니스	– 유 · 무선 기반의 다양한 멀티미디어 관련 비즈니스 – P2P, 분산형 게임, 텔레매틱스, 공장자동화 등
새로운 시장	– 고품질 콘텐츠 시장 – 홈네트워크 및 정보가전 활성화 – 유 · 무선 통합형 Post PC 형 단말기 분야

※ 자료출처 : 한국전산원 「IPv6동향2004」, 2004

[표 1-3]은 IPv4와 IPv6의 특징을 비교하여 정리한 것이다.

표 1-3 IPv4와 IPv6의 특징

구분	IPv4	IPv6
주소크기	32 bits	128 bits
주소개수	약 43억개	약[43억×43억×43억×43억]개
사용현황	전세계적으로 사용	현재 연구/실험용으로 사용, 새로운 장비는 도입개발 중
주소할당	Class 단위의 비순차적 할당 (비효율적)	네트워크 규모 및 단말기수에 따른 순차적할당 (효율적)
기본 헤더필드수	14	8
헤더 checksum	있음	기능삭제
plug&play 기능	없음	있음 (auto configuration 가능)
QoS 제어	Best Effort 방식으로 품질 보장이 곤란 (Type of Service 에 의한 QoS 일부지원)	등급별, 서비스별로 패킷 구분이 가능하여 품질보장이 용이 (Traffic Class, Flow Label 에 의한 QoS지원)
보안기능	별도의 IPSec Protocol 추가	확장기능에서 기본적으로 제공
Mobile IP 기능 적용	비효율적	효율적

IPv4에 비해 특히 구별되는 IPv6의 특징은 다음과 같다.

▶ **효율적인 헤더 포맷** : IPv4의 헤더 크기는 가변적으로 변화하지만 IPv6는 단순하고 고정된 크기의 헤더를 사용하여 패킷처리의 효율성을 높였다. 기본헤더 이외의 옵션은 확장헤더를 통해 처리한다.

▶ **확장된 주소공간** : IPv6는 주소크기가 32비트에서 128비트로 확장되어 더 많은 단계의 어드레스 계층구조와 다수의 노드를 표현할 수 있으며, 주소 자동 설정(Address Auto-configuration)

기능을 통해 사용자 편리성을 극대화하였다.

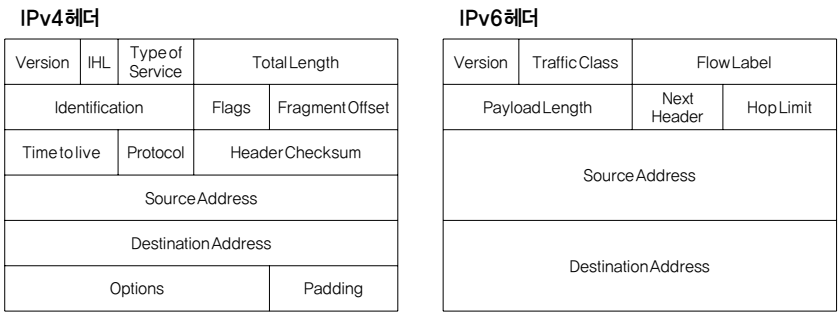
▶ QoS 지원 능력 : 플로우 레이블을 이용하여 서비스별 품질제어가 가능하게 되었다.

▶ 보안의 강화 : IPv6에서는 인증, 데이터의 무결성, 데이터의 비밀성을 제공하기 위한 IPSec 확장헤더가 필수사항이다.

1. 헤더의 변화

(그림 1-3)은 IPv4 헤더와 IPv6 헤더의 구성에 대한 차이를 보여주고 있다.

그림 1-3 IPv4/IPv6헤더 비교



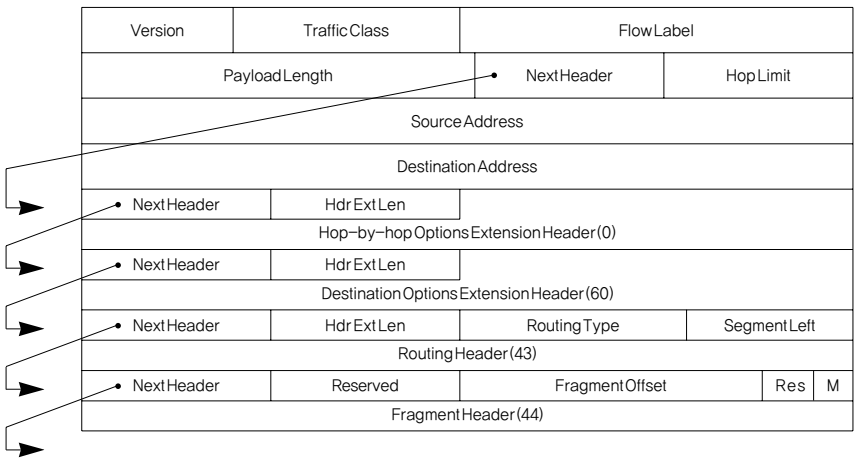
IPv6에서는 패킷의 효율적인 처리를 위해 기본헤더를 간략화하고 확장 헤더의 개념을 도입하였다. IPv6 헤더는 항상 40바이트로 고정되어 있기 때문에 IPv6에는 헤더 길이 필드가 불필요하며, 서비스 유형 필드는 IPv6 트래픽 클래스 필드로 변경되었다. 또한 전체 길이 필드가 없어지고 페이로드의 크기만 표시하는 IPv6 페이로드 길이 필드로 바뀌었다. 이러한 변화에 따른 IPv6 헤더의 특징을 요약

하면 아래와 같다.

- ▶ 헤더 길이(Internet Header Length) 필드 제거
- ▶ 서비스 유형(Type of Service) 필드는 트래픽 클래스(Traffic Class) 필드로 대체
- ▶ 전체 길이(Total Length) 필드는 페이로드 길이(Payload Length) 필드로 대체
- ▶ 식별(Identification), 플래그(Flags), 프래그먼트 옵셋(Fragment Offset) 필드는 제거
- ▶ TTL 필드는 홉 제한(Hop Limit)이라고 함
- ▶ 프로토콜(Protocol) 필드는 넥스트 헤더(next header) 필드로 대체
- ▶ 헤더 검사합(Header Checksum)은 제거
- ▶ 옵션(Option) 필드는 확장 헤더로 구현

IPv6 패킷에는 기본 헤더 뒤에 데이터의 전송에 대한 세부사항들을 필요에 따라 정의하거나 지정할 수 있도록 여러 가지 옵션들을 추가할 수 있는 확장 헤더들이 위치할 수 있다. 확장 헤더는 (그림 1-4)에서 보는 바와 같이 기본 헤더의 next header필드가 다음 확장헤더의 종류를 지시하는 형태로 구성되며, 맨 앞의 1byte가 다음 확장헤

그림 1-4 IPv6 확장헤더의 구성



더를 표시한다. 또한, 각 확장헤더는 IPv6 기본 헤더와 상위 계층 헤더 사이에 위치하며, 각 헤더의 길이는 8 옥텟의 정수배를 사용한다. 이러한 확장헤더에는 Hop-by-Hop options 헤더, Destination options 헤더 , Routing 헤더, Fragment 헤더, Authentication 헤더 등이 있다. 대표적인 확장헤더의 기능은 [표 1-4]와 같다.

표 1-4 확장헤더의 기능

확장헤더명	next header값	기능
Hop-by-Hop options	0	- 패킷 전송경로상의 모든 노드가 참조하여 처리 - option type에 따라 아래와 같은 다양한 정보를 포함할 수 있음 ① Router Alert 옵션 : 중계 라우터가 IP 데이터그램을 정밀 검사 ② Jumbo Payload 옵션 : 대용량 페이로드를 지원하기 위한 옵션
Destination options	60	- 목적지 주소의 노드만 참조하여 처리 - option type에 따라 바인딩 업데이트 확인과 같은 다양한 정보를 포함할 수 있음
Routing	43	- 발신자가 패킷의 중계 라우터를 지정하는데 사용
Fragment	44	- 패킷 분할 및 조합 정보 표현에 사용
Authentication	51	- 데이터 무결성 및 송신자 인증 정보 표현에 사용
Encapsulating Security Payload	50	- 패킷의 페이로드 영역의 암호화 정보 표현에 사용

2. 주소체계의 변화

IPv6는 IPv4의 한계성을 극복하기 위해 주소공간을 확장하였다. [표 1-5]는 IPv4와 IPv6의 주소체계를 비교한다.

IPv6는 다음과 같은 3가지 유형의 주소가 있다.

▶ 유니캐스트(Unicast) : 단일 인터페이스를 위한 식별자. 유니캐스트 주소로 전송된 패킷은 해당 주소에 의해 식별된 인터페이스로 전달한다.

표 1-5 IPv4와 IPv6의 주소체계의 비교

구분	IPv4	IPv6
주소크기	32 bits	128 bits
	약 43억개	약[43억×43억×43억×43억]개
주소표기	8비트씩 4부분으로 10진수 표기	16비트씩 8부분으로 16진수로 표기
	예) 202.30.64.22	예)2001:0230:abcd :ffff:0000:0000:ffff:1111
멀티캐스트 주소 할당	A~E의 5클래스 중 D클래스 228개 주소	주소 상위 8bits가 '1' 값인 2^{112}개 주소
	224.0.0.1 – 238.255.255.255	FFxx:0:0:0:0:0:0:0 – FFxx:F:F:F:F:F:F:F

▶ 애니캐스트(Anycast) : 인터페이스들의 집합을 위한 식별자. 해당 인터페이스들은 대부분의 경우 서로 다른 노드에 속함. 애니캐스트 주소로 전송된 패킷은 해당 주소에 의해 식별된 인터페이스들 중 라우팅 프로토콜 거리측정에 따라 가장 '가까운' 인터페이스로 전달한다.

▶ 멀티캐스트(Multicast) : 인터페이스들의 집합을 위한 식별자. 해당 인터페이스들은 대부분의 경우 서로 다른 노드에 속함. 멀티캐스트 주소로 전송된 패킷은 해당 주소에 의해 식별된 모든 인터페이스로 전달. IPv6에는 브로드캐스트 주소가 따로 존재하지 않고, 멀티캐스트의 특수한 형태로 처리한다.

IPv6 주소는 노드가 아닌 단일 인터페이스에 할당된다. 그러나 하나의 인터페이스에 여러 개의 IPv6 주소를 할당 할 수 있으므로 노드 식별은 해당 노드에 할당된 여러 개의 유니캐스트 주소를 통해 이뤄질 수 있다. 반면 IPv4 주소는 인터페이스당 한 개만이 할당될 수 있다.

IPv6 주소 중 유니캐스트에 사용되는 주소를 보다 상세히 구분하면 아래와 같다.

▶ **링크 로컬 주소**(Link-Local Address) : 링크 로컬 주소는 동일한 링크에 있는 인접 노드와 통신할 때 노드에서 사용한다. 즉, 라우터로 분리되는 세그먼트가 없는 단일 링크 IPv6 네트워크에서 호스트들은 링크 로컬 주소를 이용하여 통신할 수 있다. 링크 로컬 주소는 16진수 FE80(이진수 : 1111 1110 1000 0000)으로 시작되며, 링크 로컬 주소는 단일한 링크 내에서만 유효하므로 링크 로컬 주소를 가진 패킷은 라우터를 거쳐 다른 세그먼트로 전달될 수 없다.

▶ **글로벌 유니캐스트 주소**(Global Unicast Address) : 글로벌 유니캐스트 주소는 인터넷에서 범용적으로 사용할 수 있는 IPv6 주소 체계이다. 글로벌 유니캐스트 주소는 목적에 따라 다양한 형태의 포맷을 가질 수 있으나, 일반적으로 라우터에서 프리픽스를 제공받고, 인터페이스 자신의 고유한 ID를 참조하여 구성한다. 바로 이러한 IP 주소 구성을 통해 주소자동설정이라는 IPv6의 강력한 기능을 활용할 수 있다.

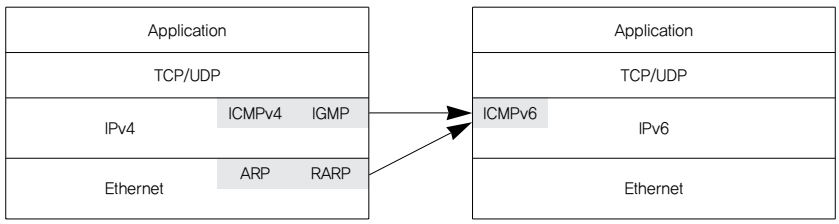
▶ **불특정 주소**(Unspecified Address) : IPv6의 불특정 주소(0:0:0:0:0:0:0:0 또는 ::)는 IPv4의 불특정 주소 0.0.0.0과 같은 개념으로 시스템을 처음 부팅하는 경우 등에 임시 주소로 사용된다.

▶ **루프백 주소**(Loopback Address) : 루프백 주소(0:0:0:0:0:0:0:1 또는 ::1)는 노드가 스스로에게 패킷을 보낼 수 있는 루프백 인터페이스를 식별하는데 사용된다. 이는 IPv4의 루프백 주소인 127.0.0.1의 개념과 동일하다.

3. ICMPv6의 도입

IPv6는 제어 프로토콜로 IPv4의 ICMPv4보다 개선된 ICMPv6를 사용한다. (그림 1-5)는 통합된 ICMPv6의 기능을 나타낸 것이다.

그림 1-5 통합된 기능의 ICMPv6



IPv4는 통신 중에 발생하는 에러와 전송경로의 변경들을 위한 정보메시지를 제어하기 위하여 ICMPv4를 사용하였다. IPv6도 동일한 이유로 ICMPv4의 기능을 확장한 ICMPv6를 사용한다. ICMPv6의 메시지도 ICMPv4에서와 같이 에러 메시지와 정보 메시지의 두 가지 카테고리로 분류할 수 있다. 에러를 표시하기 위한 메시지는 메시지 유형이 0~127 사이의 정수값을 가지며, 정보를 전달하기 위한 메시지는 128~255 사이의 값을 가진다. [표 1-6]에서는 ICMPv6의 메시지 종류를 기술하였다.

ICMPv6는 ICMPv4와 호스트의 진단을 위한 메시지 및 에러 메시지를 제공하고, 보안이 제한적이라는 유사점이 있으나, ICMPv6는 ICMPv4와는 다른 프로토콜 번호(IPv4는 '1', IPv6는 '58')를 사용한다. 또한, ICMPv6의 최대 길이는 IPv6 헤더를 포함하여 1,280 바이트로 확장되었다. [표 1-7]에서는 ICMPv6와 ICMPv4의 메시지를 비교하였다.

표 1-6 ICMPv6 메시지 종류

메시지 구분	메시지 번호	메시지종류	비고
Error	1	Destination Unreachable Error	패킷이 목적노드에 도달할 수 없는 경우
	2	Packet Too Big Error	링크의 MTU보다 패킷이 큰 경우
	3	Time Exceed Error	hop limit = 0인 패킷 수신/처리
	4	Parameter Problem Error	패킷 헤더 문제 발견
Information	128	Echo Request	특정노드의 생존여부 질의
	129	Echo Reply	특정노드의 생존여부 응답
Group Membership	130	Group Membership Query	
	131	Group Membership Report	
	132	Group Membership Termination	
Router Discovery	133	Router Solicitation(RS)	RA 메시지의 요청
	134	Router Advertisement(RA)	– RS의 응답으로 또는 주기적 송신 – 라우터의 정보 포함
Neighbor Discovery	135	Neighbor Solicitation(NS)	NA 메시지의 요청
	136	Neighbor Advertisement(NA)	– NS의 응답으로 또는 필요시 송신 – 호스트의 정보 포함
Redirection	137	Redirection	목적노드까지의 최적 경로를 알려줌
Router Renumbering	138	RR	라우터상의 프리픽스 재설정에 사용
Name Lookup	139	Name Information Query	
	140	Name Information Reply	

표 1-7 ICMPv6와 ICMPv4 메시지 비교

메시지 종류	IPv4	IPv6	비고
Echo request and reply	O	O	
Timestamp request and reply	O	×	사용되지 않는 기능으로 삭제됨
Address mask request and reply	O	×	사용되지 않는 기능으로 삭제됨
Router solicitation	O	O	
Neighbor solicitation	ARP	O	ICMPv6 기능으로 통합
Group membership	IGMP	O	ICMPv6 기능으로 통합
Destination unreachable	O	O	
Source quench(socket buffer full 표시)	O	×	사용되지 않는 기능으로 삭제됨
Packet too big	×	O	링크의 MTU보다 패킷이 큰 경우
Time exceeded	O	O	
Parameter problem	O	O	
Redirection	O	O	

4. NDP(Neighbor Discovery Protocol) 사용

NDP는 호스트가 연결된 링크상의 라우터 탐색, 프리픽스 정보 탐색, MTU와 같은 인터넷 파라미터 정보의 탐색, 호스트 주소의 자동 설정 등의 동일 링크에 연결된 노드간의 상호작용에 관련한 문제들을 해결하기위해 사용된다. 또한, NDP는 IPv4의 ARP(Address Resolution Protocol)의 기능도 포함하며, [표 1-8]과 같은 ICMPv6 정보메시지를 이용한다.

표 1-8 NDP 메시지 종류

메시지 종류	특징
Router Solicitation/Advertisement	– 자신과 동일한 링크에 연결되어 있는 라우터를 파악할 때 사용 – 호스트는 Router Solicitation 으로 질의를 전송 – 라우터는 Router Advertisement로 자신의 정보를 전달
Neighbor Solicitation/Advertisement	– IPv4에서의 ARP기능 – 노드는 Neighbor Solicitation으로 질의를 전송 – Neighbor Solicitation을 수신한 노드는 Neighbor Advertisement로써 응답
Redirect	– 라우터가 더 나은 경로를 알고 있을 때 Redirect 메시지를 패킷의 소스에게 전달

5. 주소 자동 설정 (Address Auto-configuration) 기능사용

IPv6에서는 ICMPv6를 활용해서 호스트의 주소와 디폴트 라우터를 자동으로 설정할 수 있다. 이러한 IP 주소 자동 설정 기능은 IPv6의 새로운 기능 중 하나로, 각종 단말에 IPv6 주소가 자동적으로 생성되도록 한다. 이 기능을 이용하면 일반 PC 뿐만 아니라 콘솔이나 디스플레이가 없는 Embedded OS 및 non-PC 장치까지 IPv6 주소를 부여할 수 있으므로, 사용자는 별도의 IPv6 주소를 설정할 필요가 없으며, 관리자 또한 사용자 별로 IP 주소를 할당해야하는 관리상의 불편함을 줄일 수 있다.

주소 자동 설정 기능을 이용하는 호스트는 라우터로부터 주소를 비롯한 모든 네트워크 정보를 받을 수도 있고, 또는 주소 정보만을

받고 나머지 네트워크 정보들은 DHCP 서버로부터 받을 수도 있다.

[표 1-9]에서는 상태형 주소 자동 설정(Stateful Addesses Auto-configuration)과 비상태형 주소 자동 설정(Stateless Addresses Auto-configuration)를 구분하여 설명하였다.

표1-9 주소 자동 설정 방법

구분	특징
Stateful Address Auto-configuration	- 외부 서버 이용(DHCPv6)
Stateless Address Auto-configuration	- NDP 메시지를 이용하여 자동 설정 - Link-local 주소를 NDP메시지의 IPv6 헤더에 사용 - Prefix, default router, address duplication 여부 파악

6. 보안 기능의 강화

IPv4에서는 보안 기능이 필요한 경우 IPSec을 따로 설치하여 사용해야 했으나, IPv6에서는 IPSec을 기본적으로 내장하여 보안을 강화하였다. IPv6의 IPSec은 프로토콜 자체에 내장된 확장 헤더를 이용하기 때문에, 별도의 프로그램이나 모듈을 설치할 필요가 없어 보안 기능의 필요성과 망 효율성에 따라 비교적 쉽게 추가 또는 제거될 수 있는 특징을 가진다.

IPSec은 데이터의 보안을 위해 AH 및 ESP 프로토콜을 사용한다. AH 프로토콜은 무결성, 데이터 소스 인증 및 재생 공격 방지에 사용된다. ESP 프로토콜은 데이터의 기밀성을 제공하기위해 암호화되어 있지만 인증되지 않은 데이터 스트림에 대한 공격을 막기 위해 AH의 모든 기능이 포함돼 있다. 각 프로토콜은 전송모드와 터널모드를 지원한다. 전송 모드는 종단간에 위치한 호스트들 사이에서 이용되며 IP 패킷의 페이로드, 즉, TCP와 UDP와 같은 상위계층 프로토콜 데이터만을 보호한다. 터널 모드의 경우는 원래 패킷의 전체가 보호 영역 안에 놓이므로, 데이터의 기밀성도 유지할 수 있다. 보안 통신의 한 쪽이 호스트가 아닌 라우터 (통상, 어떤 인트라넷의 Security Gateway에 해당됨)인 경우는 반드시 터널 모드를 적용해야 하며, 호스트- 호스트 간에도 적용할 수 있다.

제 2 장 IPv6의 보안취약성 및 대응방안

본 장에서는 IPv6네트워크를 유선 환경과 이동 환경으로 구분하여 보안취약성 및 대응방안에 대해 살펴보도록 한다. 유선 환경에서는 패킷 헤더, 주소설정 및 라우팅 동작과정 등에서 발생할 수 있는 보안취약성 및 그에 대한 대응방안에 대하여 기술한다. 또한, 이동 환경에서의 노드 이동성을 지원하는 기술에 대한 보안취약성 및 대응방안을 살펴보도록 한다.

제 1 절 유선 환경에서의 IPv6 보안취약성 및 대응방안

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

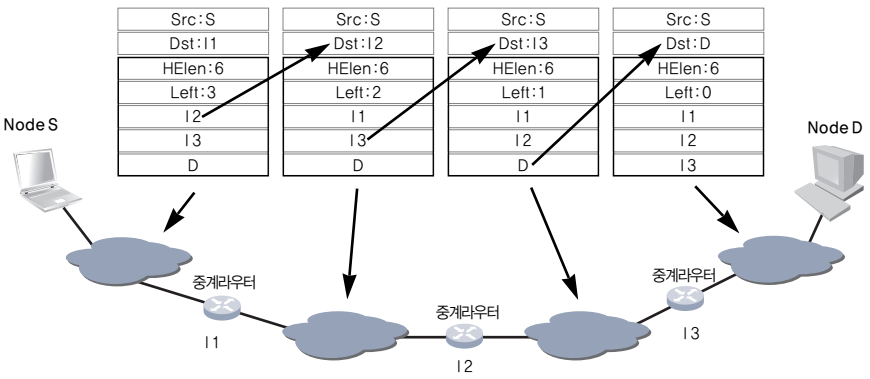
- ▶ IPv6의 확장된 주소 범위로 인해 취약한 호스트를 찾기 위한 포트 스캐닝이 어렵다는 장점이 있는 반면에 공격자를 추적하기 어려움
- ▶ 침입차단시스템과 침입탐지시스템은 IPv6의 새로운 기능 및 보안 기능 처리를 위한 CPU 오버헤드로 인해 서비스거부공격 가능성이 높음
- ▶ 라우팅 헤더 등의 확장 헤더를 악용하여 침입차단시스템을 우회할 수 있음
- ▶ 공격자는 IPv6 주소 자동 설정 기능을 악용하여 정상적인 주소 할당을 방해하거나 정상적인 세션을 종료할 수 있음

1. 소스 라우팅을 위한 라우팅 헤더

가. 보안취약성

IPv6 라우팅 헤더는 패킷이 목적지까지 경유하는 중계 라우터들을 송신자가 지정하는데 사용된다.

그림 2-1 라우팅 헤더의 동작

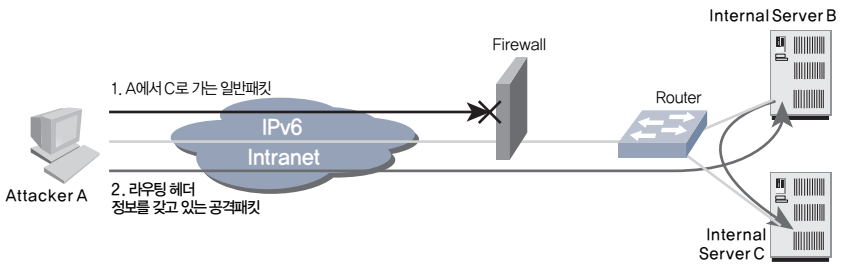


(그림 2-1)은 라우팅 헤더의 동작을 보여준다. 단, 라우팅 헤더내의 'type' 필드 값이 0인 경우에만 라우팅 헤더의 네트워크 주소 목록이 포함된다. 패킷이 발신지에서 전송될 때, IP 헤더의 목적지 주소는 전송되는 경로의 첫 번째 중계 라우터를 가리킨다. 라우팅 헤더의 목록은 경로를 따라 다음의 중계 라우터를 나타낸다. 패킷이 각각의 라우터에 도착할 때마다, 해당 라우터는 패킷의 목적지 주소를 네트워크 주소 목록의 다음 중계 라우터로 변경한다.

(그림 2-2)에서 침입차단시스템의 접근제어 규칙에 의해 공격자 A가 내부 서버 B에는 접근이 가능하나, 내부 서버 C에는 접근할 수 없도록 설정되어 있다고 가정한다. 이 때의 취약성은 다음과 같다.

접근 가능한 내부 서버 B의 라우팅 헤더 처리가 가능하고 라우팅 헤더의 'Segments Left' 필드 값이 1 이상인 경우에 공격자 A는 내

그림 2-2 라우팅 헤더 보안취약성



구분	송신자	최종 목적지	목적지 포트번호	라우팅 헤더 'Segs Left' 필드값	라우팅 헤더 'Address' 필드값
1	A	B	53	1	C
2	A	C	53	0	B

부 서버 B를 경유하여 공격자가 직접 접근할 수 없는 내부 서버 C로 공격 트래픽을 전달할 수 있다. 따라서 라우팅 헤더를 이용하면 목적지 주소 기반의 접근 제어를 하는 침입차단시스템의 필터링을 우회할 수 있다.

나. 대응방안

이와 같은 보안취약성에 대한 대응 방안은 다음과 같다.

- ▶ 침입차단시스템은 type 필드 값이 0인 라우팅 헤더를 갖는 패킷을 차단하도록 필터링 규칙 설정
- ▶ 침입차단시스템은 최종 목적지 주소와 라우팅 헤더의 'Address' 필드 값을 비교할 수 있는 필터링 규칙 설정
- ▶ 호스트는 수신된 패킷의 라우팅 헤더에 포함된 최종 목적지 주소가 자신의 주소가 아닌 경우에는 패킷을 폐기

2. 사이트 범위(Site-Local scope)를 갖는 멀티캐스트 주소

가. 보안취약성

IPv6에서는 브로드캐스트 주소 대신에 멀티캐스트 주소를 이용하여 브로드캐스트 서비스를 제공한다. [표 2-1]과 같이 모든 라우터 및 DHCP를 지정하는 주소를 제공하고 있으며, 공격자는 모든 라우터를 나타내는 (FF05::2) 주소와 모든 DHCP서버를 나타내는 (FF05::1:3) 주소를 목적지 주소로 사용하여 플러딩 공격(Flooding Attack)을 할 수 있다.

표 2-1 모든 라우터 및 DHCP 서버를 지칭하는 IPv6 멀티캐스트 주소

사이트 범위를 갖는 멀티캐스트 주소	의 미
FF05::2	모든 라우터를 지칭
FF05::1:3	모든 DHCP 서버를 지칭

(그림 2-3)에서는 IPv6의 멀티캐스트 주소를 이용하여 공격할 라우터에 대한 스캔작업 없이 모든 라우터에 대한 서비스거부공격을 하는 것을 보여준다.

또한, IPv4 환경에서는 공격자가 취약한 시스템을 찾기 위해 [표 2-2]에서와 같이 네트워크상의 (2^8=256)개 호스트들에 대해 무작위적인 스캔을 수행해야 한다.

그림 2-3 멀티캐스트 주소를 이용한 공격

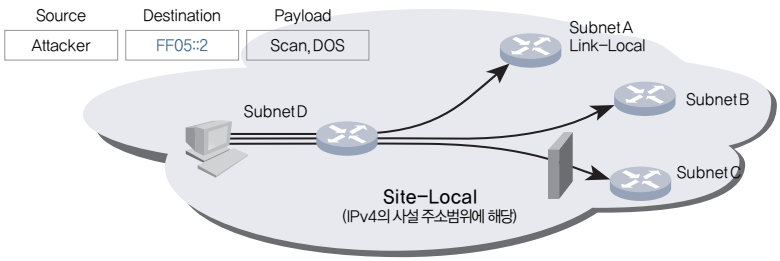


표 2-2 IP 버전에 따른 서브넷의 크기

IP 버전	서브넷의 크기
IPv4	8bit 크기의 서브넷 주소 사용이 일반적(2^8개 host)
IPv6	64bit 크기의 서브넷 주소 사용(2^{64}개 host)

반면에, IPv6 환경에서는 최대 2^{64}개의 호스트들을 스캔해야 하므로 공격자는 스캔해야 할 범위를 줄이기 위해 다음과 같은 보안취약성을 이용할 수 있다.

▶ 관리자는 할당할 수 있는 많은 주소 공간이 있음에도 불구하고 관리상의 이유로 각 노드들에 대해 기억하기 쉬운 주소를 사용할 경우 공격자는 작은 범위의 주소 공간에 대한 스캔으로 다른 노드들도 유추할 수 있음

▶ 공격자는 IEEE EUI-64 주소의 고정 부분을 이용하여 작은 범위의 주소 공간에 대한 스캔으로 다른 노드들도 유추할 수 있음

▶ 이더넷 카드 제조 회사의 정보를 이용하여 인터페이스의 주소 범위 추측이 가능함

나. 대응방안

이러한 공격을 막기 위해서는 외부로부터 멀티캐스트 주소에 접근할 수 없도록 네트워크 경계 지역의 침입차단시스템 및 침입탐지시스템에서 필터링을 수행하여야 한다. 또한 아래와 같은 조치를 통해서 스캔을 포함한 공격의 위험을 경감시킬 수 있다.

▶ 경계 라우터에서 내부(internal-use) IPv6 주소 필터링

▶ 주요 시스템에는 추측이 어려운 IPv6 주소를 할당 사용

▶ 불필요한 ICMPv6 메시지 유입/유출 차단

▶ 침입차단시스템은 최소한의 링크 로컬 멀티캐스트(link-local multicast) 트래픽만을 허용(FF02::/10)

▶ 침입차단시스템은 IPv6 멀티캐스트 주소와 ICMPv6 메시지를 처리할 수 있어야 하며 각각의 메시지에 대한 필터링을 적용

▶ 침입차단시스템과 경계 라우터는 사이트 범위의 목적지 주소를 갖는 패킷 유입을 차단

▶ 노드가 사이트 범위 내의 적법하지 않은 멀티캐스트 그룹에 가입하는 것을 방지

따라서, IPv6 멀티캐스트 서비스 중 SSM(Source-Specific Multicast) 가입 요청이 정상 메시지인지 공격 메시지인지를 구분할 수 있도록, 멀티캐스트 주소에 대한 적합한 필터링 규칙을 적용해야 한다.

3. 통합된 ICMPv6

가. 보안취약성

'Destination Unreachable' 에러 메시지는 네트워크의 정체에 의해 버려진 패킷에 대해서는 생성되지 않으며, 그 외 다른 이유로 목적지 노드에 도달할 수 없는 패킷에 대해 생성된다. 에러 메시지는 송신자가 속한 라우터 또는 목적지 노드에서 생성된다.

이와 같이 ICMPv6은 처리가 불가능한 특정 패킷들이 멀티캐스트 주소로 전송되면 에러 메시지를 송신자에게 보내는 것을 허용함으로써, 다음과 같은 취약성을 갖는다.

▶ 수신한 패킷의 크기가 'next link MTU' 보다 큰 경우에는 멀티캐스트 트래픽에 대한 'Path MTU Discovery'를 지원하기

위해 'packet too big' 이라는 응답메시지를 전송하는데 이를 악용한 서비스거부공격에 취약함

▶ hop-by-hop 또는 Destination Options 확장헤더에 옵션 값이 잘못 설정된 패킷을 수신할 경우에는 'parameter problem' 응답메시지를 전송하는데 이를 악용한 서비스거부 공격에 취약함

또한, 공격자가 ICMPv6메시지 중 RS(Router Solicitation)와 RA(Router Advertisement)메시지를 위조하여 잘못된 Prefix 정보를 내부 네트워크에 전파할 수 있다.

나. 대응방안

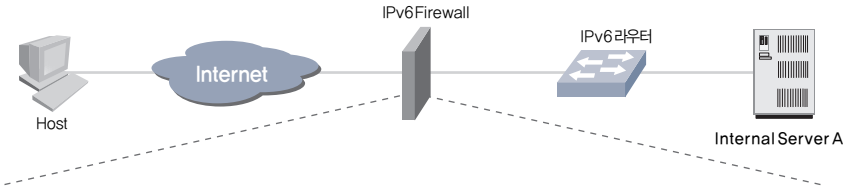
ICMPv6에 대한 침입차단시스템의 보안 정책[(그림 2-4)참조]과 ICMPv4에서의 보안 정책[(그림 2-5)참조]은 달라야 한다. IPv6에서는 목적지나 목적포트에 대한 필터링뿐만 아니라 확장헤더에 대한 필터링이 가능하여야 한다. 또한, 침입차단시스템이 neighbor discovery protocol 및 neighbor solicitation protocol의 처리를 지원하고, 동적 라우팅 프로토콜을 필터링 할 수 있어야 하며, 다양한 인터페이스 타입을 지원할 수 있어야 한다.

RS와 RA의 보안취약성에 대한 대응방안으로 RFC2461[1]에서는 IPSec AH 이용을 제안하고 있으나, IPSec 자동 키(automatic keying) 설정의 문제로 인해 수동 키(manual keying) 설정 방식만 가능하다. 또 다른 대응방안은 SEND 워킹그룹에서 제안한 것으로 공개키 서명 방식과 CGA(Cryptographic Generated Address)를 사용하는 방식이 있다. CGA는 제공되는 보안 강도가 높고 절차가 간단하지만 각 노드에서 처리해야 하는 암호학적 연산의 양이 많아지므로 일반적으로 성능이 낮은 이동 단말에서는 적용하기 어렵다.

IPv6 환경에서는 목적지 주소가 멀티캐스트 주소인 경우 응답메

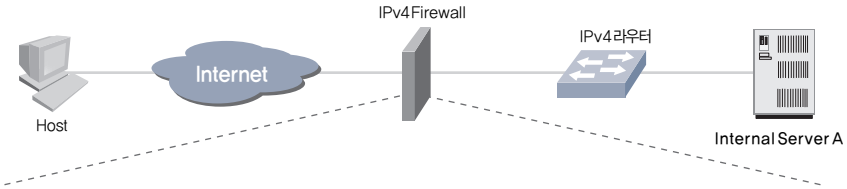
1) Neighbor Discovery for IP Version 6 (IPv6), IETF

그림 2-4 ICMPv4에 대한 필터링 규칙



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet too Big
Permit	Any	A	3	0	Time Exceeded-TTL Exceeded

그림 2-5 ICMPv4에 대한 필터링 규칙



Action	Src	Dst	ICMPv4 Type	ICMPv4 Code	Name
Permit	Any	A	0	0	Echo Reply
Permit	Any	A	8	0	Echo Request
Permit	Any	A	3	0	Dst. Unreachable-Net Unreachable
Permit	Any	A	3	4	Dst. Unreachable-Frag. Needed
Permit	Any	A	11	0	Time Exceeded-TTL Exceeded

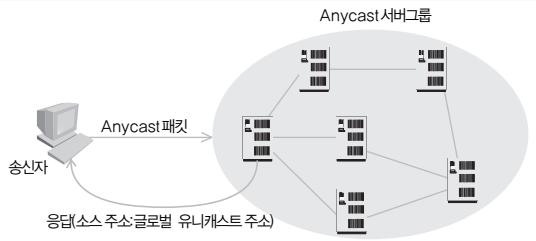
시지를 생성하지 않도록 하여 Smurf 공격을 방지할 수 있도록 하고 있다. 그러나, 'Packet Too Big' 메시지, 'Parameter Problem' 메시지인 경우는 예외적으로 응답을 허용하고 있으므로 항상 트래픽 모니터링을 통해 서비스거부공격 여부를 감시해야 한다.

4. 최적의 서비스 탐색을 위한 애니캐스트

가. 보안취약성

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((그림 2-6) 참조).

그림 2-6 애니캐스트를 이용한 통신



인증되지 않은 애니캐스트 그룹 멤버가 거짓 정보를 광고하거나 해당 멤버에 의해 송신자의 주소를 변경할 수 있는 보안취약성으로 인하여, 위장공격(Masquerading) 및 서비스거부공격이 가능하다.

나. 대응방안

이를 위한 대응 방안으로서 (그림 2-7)와 같이 외부에서의 애니캐스트 서비스 요청을 제한하기 위해 침입차단시스템은 사용되는 애니캐스트 주소를 필터링을 해야 한다.

또는 (그림 2-8)과 같이 IPSec 및 IKE(Internet Key Exchange protocol)를 애니캐스트에 적용하여 보안통신채널을 사용해야 한다.

그림 2-7 침입차단시스템을 이용한 패킷 필터링

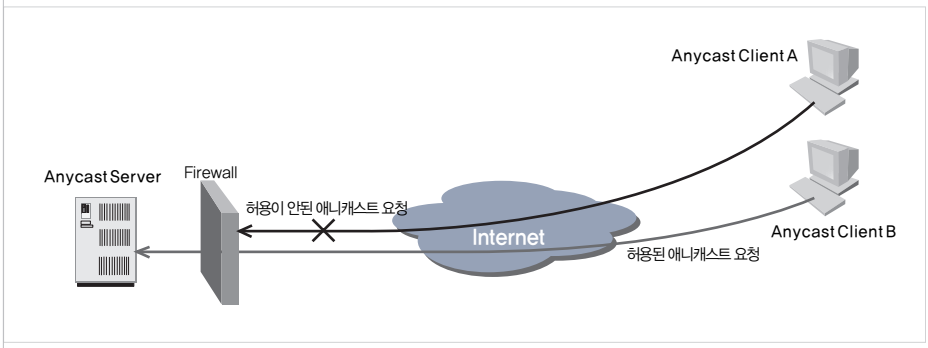
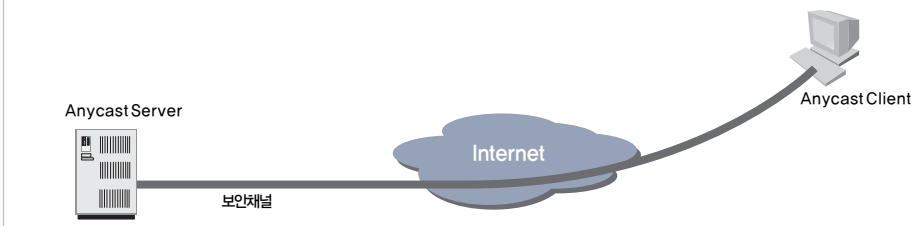


그림 2-8 통신보안 채널 설정을 통한 통신



5. 동적 주소설정을 위한 프라이버시 확장

가. 보안취약성

프라이버시 확장(privacy extensions)은 인터페이스 식별자를 변경하여 호스트의 IPv6주소가 스캔 위협에 노출되는 것을 방지하는 목적으로 사용된다. 반면에 공격자의 인터페이스 식별자 변경이 용이하여 침해사고 시 공격자에 대한 추적 및 호스트의 관리가 어려워질 수 있다.

호스트가 주소를 할당 받기 위해 수동설정이나 DHCP를 통하는 경우에는 DNS에 주소를 등록하는 것이 제한적이나 주소 자동 설정을 이용하면 DDNS(Dynamic DNS)를 통해 동적으로 주소를 등록할 수 있다. 이로 인해 공격자가 자신의 주소를 용이하게 변경할 수 있

어 분산서비스거부공격에 대한 방어가 어려울 수 있다. 또한 주소 자동 설정에 프라이버시 확장을 사용하면 DDNS의 업데이트 작업의 오버헤드가 발생하여 가용성이 떨어질 수 있다.

나. 대응방안

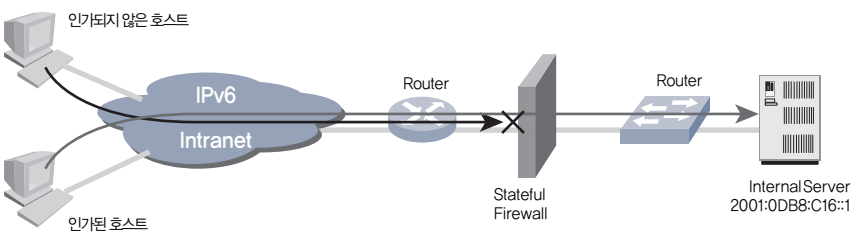
이를 해결하는 방안은 주소 설정을 위한 노드와 DDNS 서버 간 SA(Security Association)를 통하여 인증된 노드만이 주소 갱신을 하도록 하며 프라이버시 확장을 사용하는 노드는 주소 업데이트 주기에 대한 적절한 값을 설정해야 한다.

6. IPv6 주소 및 포트 정보를 이용한 접근제어

가. 보안취약성

IPv4와 마찬가지로 IPv6 기반의 침입차단시스템은 접근제어 기능을 사용하여 인증된 호스트만 내부 네트워크로 접속할 수 있게 한다. 그러나 (그림 2-9)에서와 같이 IPv6 노드는 다중 주소를 가질 수 있기 때문에 주소와 라우팅을 고려한 보안 정책이 필요하다.

그림 2-9 다중 주소에 따른 필터링 문제



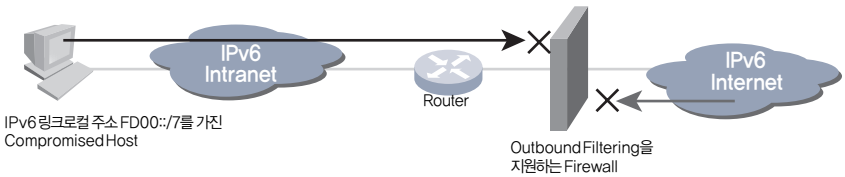
Action	Src	Dest	Src Port	Dst Port
Permit	2001:0DB8:C18::1	2001:0DB8:C16::1	Any	ssh
Deny	Any	Any		

IPSec 터널링을 이용하는 경우 IPv6 메시지가 암호화 되어 전송되기 때문에 메시지의 내용을 확인할 수 없어 필터링의 적용이 곤란하며 공격자는 이를 악용하여 공격패킷을 암호화하여 전송함으로서 침입차단시스템을 통과할 수 있다.

나. 대응방안

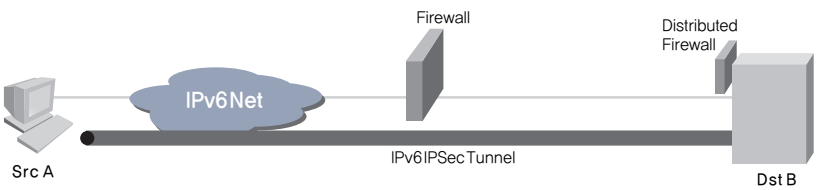
(그림 2-10)과 같이 IPv6는 하나의 인터페이스에 다중 주소가 허용되므로 침입차단시스템에서는 글로벌 주소에 대해서는 허용하고, 링크 로컬 주소에 대해서는 외부로 나가는 것과 외부에서의 접근을 막아야 한다.

그림 2-10 주소범위에 따른 필터링



Action	Src	Dest	Src Port	Dst Port
Deny	FD00::/7	Any		
Deny	Any	FD00::/7		

그림 2-11 침입차단시스템의 상위계층 정보분석



Src A Dst B	ESP HDR	Encrypted Data		Firewall 검사어려움
Src A Dst B	UDP HDR	Data		Distributed Firewall 검사가능
Src A Dst B	AH HDR	UDP HDR	Data	Firewall 검사가능

IPSec터널링 사용 시에 발생하는 패킷 접근제어 취약성을 해결하기 위한 방안으로는 암호화된 패킷을 복호화할 수 있는 분산형 침입차단시스템의 사용과 AH만 적용한 암호화 패킷 사용을 들 수 있다. (그림 2-11)과 같이 AH만 적용한 패킷은 침입차단시스템이 상위 계층의 정보를 기초로 패킷에 대한 접근제어를 하도록 한다.

7. IPv6 확장헤더

가. 침입차단시스템에서 확장 헤더 처리

IPv6 침입차단시스템은 특정 헤더와 옵션 사용에 대한 보안정책을 강화하기 위해 사용되며, 알려지지 않은 옵션을 가진 패킷들을 처리하기 위해 패킷 내 모든 확장 헤더들을 검사해야 한다.

RFC2460[2)]에서는 목적지 옵션(Destination Option)을 가진 패킷을 목적지에서만 처리되도록 하고 있으나, 중간 노드들은 인식하지 못하는 헤더나 목적지 옵션을 가진 패킷을 폐기할 수 있다.

나. 확장 헤더 체인 처리

침입차단시스템의 경우 확장 헤더를 포함한 헤더 체인은 처리할 수 없지만, 전송 PDU를 찾기 위해서는 헤더파싱이 필요하다. 이러한 점은 침입차단시스템에서 보안을 적용하는데 제한을 갖게 하고 확장 헤더 사용을 어렵게 한다.

다. Unknown 헤더/목적지 옵션 과 보안 정책

강력한 보안 정책은 unknown 헤더들 또는 목적지 옵션들을 갖는 패킷들을 침입차단시스템이나 필터링에 의해 폐기되게 한다. 즉, 침입차단시스템은 모든 확장 헤더 체인을 처리하며 unknown 헤더를 갖는 패킷을 폐기한다. 따라서 침입차단시스템이 인식하지 못하는 적법한 헤더를 갖는 패킷을 폐기하는 것을 방지하는 보안정책이 필요하다.

2) Internet Protocol, Version 6 (IPv6) Specification

라. hop-by-hop 옵션 헤더 남용

hop-by-hop 옵션 헤더는 중계 라우터가 확인해야하는 선택적 정보를 전달하는데 사용된다. 경로상의 모든 중계 라우터는 hop-by-hop 옵션 헤더를 조사하고 처리해야 한다. 그러나 IPv6는 hop-by-hop 옵션의 수를 제한하지 않으므로 경로상의 모든 중계 라우터들에 서비스거부공격을 가능하게 하는 보안취약성이 있다.

마. router alert option 남용

router alert option은 hop-by-hop option 헤더 내에 지정되어 중계 라우터들이 패킷을 정밀하게 검사하게 한다. 이러한 기능은 공격자가 서비스거부공격을 가능하게 하는 취약성을 갖게 하며, 공격자가 router alert option을 갖는 패킷을 대량으로 전송하여 라우터의 정상적인 트래픽 처리를 어렵게 한다.

8. 전송 패킷의 단편화(Fragmentation)

IPv6에서는 단편화 과정이 IPv4와는 달리 단말 호스트에서만 이루어진다. (그림 2-12)에서와 같이 Next Header가 44인 Fragment 헤더는 Fragment Offset, Identification 필드 등으로 구성된다.

그림 2-12 Fragmentation 헤더 형식

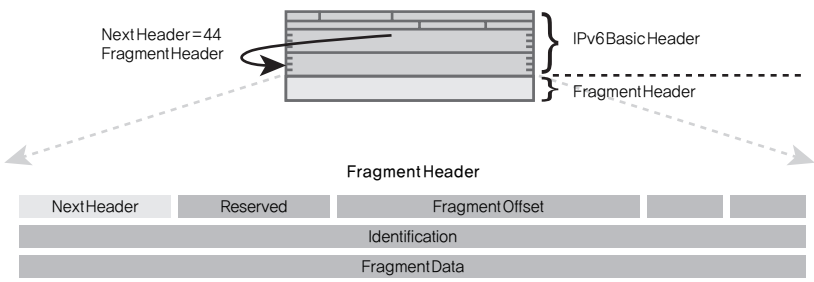
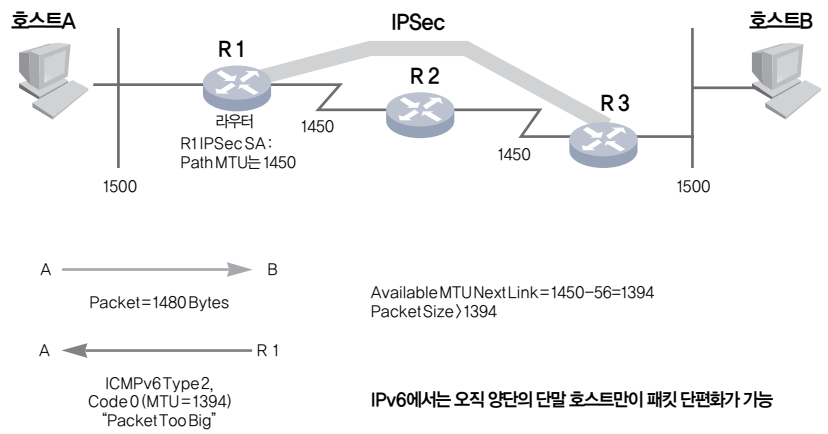


그림 2-13 패킷 단편화 과정



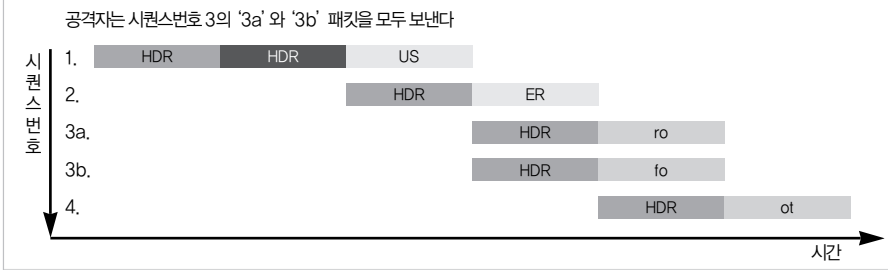
(그림 2-13)은 1480바이트 크기의 패킷을 A에서 B로 전송하는 예이다. 전송경로상의 R1은 1450바이트 이하의 패킷만을 처리할 수 있으므로, 'ICMP packet too big' 메시지를 A로 전송하여 MTU 사이즈를 1450바이트로 재조정하게 한다.

IPSec을 사용할 경우에는 터널에 사용되는 56바이트의 코드를 제외하고 실제로 전송할 수 있는 데이터 크기는 1394바이트이다. 그러므로 A는 데이터를 1394바이트 크기로 분할하여 전송해야 한다.

여기서 Path MTU는 현재 두 호스트간 경로에서 보낼 수 있는 MTU 값을 말한다. 라우팅 경로가 매번 일정하지 않고 수시로 바뀌므로 Path MTU도 라우팅 경로에 따라 수시로 변경될 수 있다. 그리고 같은 호스트 사이라 하더라도 두 호스트간의 트래픽 종류에 따라 그 값이 달라질 수 있다.

공격자의 패킷에 대한 중복되는 단편화가 침입차단시스템에서 필터링 없이 목적지까지 전송하게 되면 목적지에서 패킷의 내용이 변경될 가능성이 있다.

그림 2-14 단편화 패킷 중복 공격



(그림 2-14)는 공격자가 단편화 패킷의 일부 ' fo' 를 중복하여 보내는 예이다. 침입차단시스템이 중복된 단편화 패킷(3a, 3b)을 필터링하지 못한다면, 최종 목적지의 호스트는 분할된 패킷을 재조합(reassembly)할 때 중복된 단편화 패킷 중 어떤 패킷이 올바른 것인지 판단할 수 없게 된다. 이로 인해 시스템의 교착 상태나 충돌이 발생하여 시스템 재시동과 같은 문제를 초래할 수 있다.

이러한 위협에 대응하려면 침입차단시스템이 단편화 패킷을 재조합하여 필터링을 적용할 수 있어야 한다.

9. IPv6 라우팅

가. 보안취약성

IPv6에서는 NDP를 이용하여 네트워크 상의 라우터를 찾아내거나, prefix등을 결정할 수 있다. NDP에서 사용되는 메세지는 확인절차 없이 옳다고 간주되기 때문에 악의를 가진 노드들이 ICMPv6 확장 헤더의 옵션 필드에 거짓 정보를 넣어서 전송할 수 있다. 이로 인해 NDP를 악용하여 라우팅 정보를 변경하거나 악의를 가진 노드가 네트워크 상의 기본 게이트웨이의 역할을 함으로써 트래픽 전달을 방해할 수 있다.

나. 대응방안

IPv6에 기본적으로 탑재된 IPSec을 사용하면 NDP 메시지 변조,

가로채기를 방지할 수 있으며 DHCPv6 서버를 활용하여 보안이 취약한 NDP의 기능을 대체할 수도 있다.

또한, ff02::2 주소를 이용한 질의를 통해 네트워크에 존재하는 허위 라우터를 식별할 수 있다.

10. DNSv6

가. 보안취약성

DNS 서비스는 UDP 기반의 네트워크 서비스를 제공하고 있기 때문에 패킷 검증에 대한 메커니즘이 이루어지지 않는다. 이로 인해 피싱등의 스푸핑 공격에 의해 전송되는 패킷의 위조와 변조를 기반으로 전체 DNS 서비스의 기능을 마비시키거나 DNS 서버의 정보를 유출시키기 위한 공격의 목표가 될 수 있다.

이러한 DNS 서버에 대한 공격 형태로는 서비스 거부공격(DoS: Denial of Service) 혹은 분산 서비스 거부 공격(DDoS: Distributed DoS)을 통한 네임 서버의 기능 마비나, 공격자에 의해 피 공격자의 캐쉬에 특정 정보를 위?변조하여 악의적인 데이터를 공급함으로서 잠재적으로 DNS 이름을 기반으로 하는 뒤이은 서비스를 무력화 시키는 '캐쉬 포이즌(Cache Poisoning)' 공격이 있다. (그림 2-15)와 (그림 2-16)는 각 공격에 대한 시나리오를 나타낸 것이다.

그림 2-15 스푸핑 공격

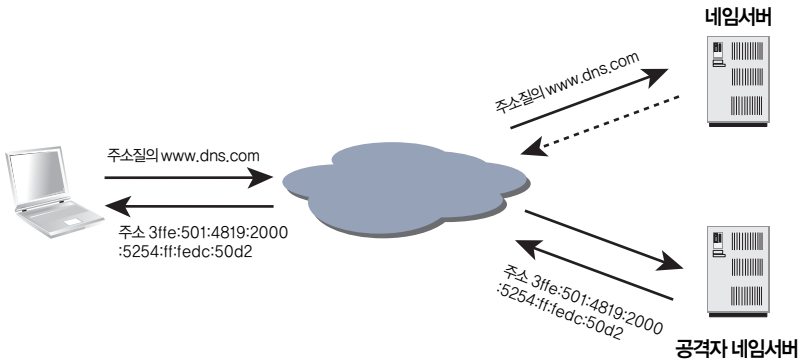
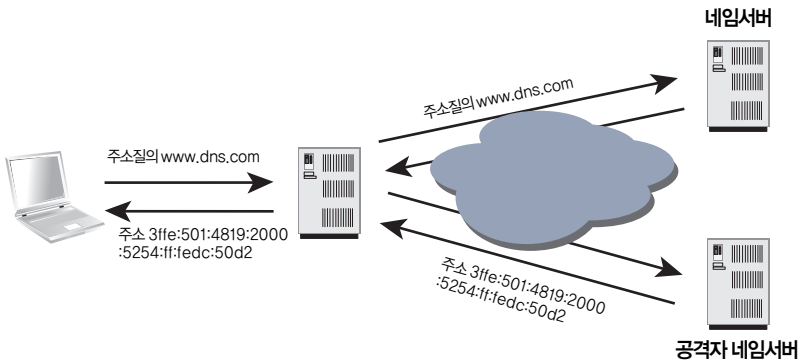


그림 2-16 DNS 캐쉬 포이즌 공격



나. 대응방안

DNSv6의 보안 공격의 위협에 대해 DNS에서 전송 데이터에 대한 위조, 변조에 대한 무결성(integrity)을 제공할 수 있는 대응방안이 필요하다. 또한 위장된 DNS서버나 호스트로부터의 위 · 변조 공격과 같은 취약성에 대해서 데이터에 대한 기원 인증(data origin authentication)과 같은 메커니즘을 사용할 수 있다.

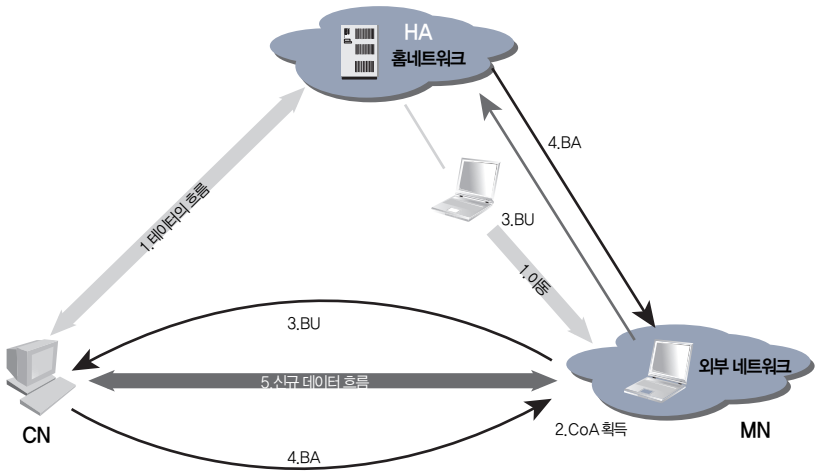
MIPv6는 IPv6에 이동성을 제공하기 위한 프로토콜로 [표 2-3]에서 MIPv6의 구성요소 및 정의를 나타내고 있다. MIPv4와 달리 FA(Foreign Agent)가 존재하지 않아, FA기반의 CoA 주소를 할당받지 않고 DHCP서버 또는 IPv6기반의 주소설정 방식에 의해 CoA를 설정한다.

표 2-3 MIPv6 구성 요소 및 용어 정의

MIPv6 구성 요소		용어 정의
MN(Mobile Node)		자신의 Network Access Point를 바꾸는 호스트 및 라우터
CN(Correspondent Node)		MN과 통신하고 있는 호스트 및 라우터
HN(Home Network)		MN이 이동하기 전에 Home-Link의 Prefix를 따르는 홈 주소를 참조하여 통신하고 있던 네트워크
HA(Home Agent)		MN의 HN에 있는 라우터 중 MN의 등록 정보를 가지고 있어 MN이 HN을 떠나 있을경우 MN의 현재 위치로 패킷을 보내주는 라우터
CoA(Care of Address)		MN이 외부 네트워크로 이동하였을 경우 IPv6의 주소자동설정으로 획득한 주소로MN이 현재 위치한 네트워크의 Prefix 정보를 갖으며, MN에서 전송하는 모든 패킷은 이 주소를 IPv6 헤더의 주소로 설정
Binding	Update(BU)	MN이 외부 네트워크로 이동하였을 경우, 자신의 HA와 CN에게 새로이 생성한 CoA를알리는 바인딩 업데이트메시지
	Request(BR)	바인딩 유효시간이 지난 후, MN으로부터 바인딩 업데이트메시지가 오지 않을 경우,CN 또는 HA의 바인딩 업데이트의 요청메시지
	Acknowledgement(BA)	바인딩 업데이트가 성공한 후, 보내는 확인메시지

이동노드 MN은 (그림 2-17)과 같이 자신의 홈네트워크에서 CN으로부터 데이터를 전달 받으며 외부 네트워크로 이동시(1)에는 라우팅 최적화 과정을 통해 옮겨진 외부 네트워크로 데이터를 전달(5)받는다. MN이 다른 네트워크로 이동 후 세부적인 동작과정은 다음과 같다. 외부네트워크로 이동한 MN이 해당 네트워크에서 CoA를 획득(2)하고, BU메시지를 통해 CoA를 HA와 CN에게 알린다(3). CN과

그림 2-17 MIPv6의 동작



· BA(Binding Acknowledgement) : 바인딩 ACK 메시지
· CoA(Care-of-Address) : 외부주소
· BU(Binding Update) : 바인딩 업데이트 메시지
· HA(Home Agent) : 홈 에이전트

HA는 CoA로의 바인딩 캐시를 갱신 후 MN에게 BA메시지를 보냄(4)으로써 갱신과정을 마치고 CN에서 MN까지 새로운 CoA를 목적지 주소로 하여 패킷이 전달(5)된다.[3)]

MIPv6는 기본 IPv6 기능의 확장이기 때문에 데이터 보안의 측면에서 적어도 기본 IPv4 또는 IPv6 만큼의 보안성을 제공할 수 있어야 하며 IPv6에 대한 새로운 보안취약성을 만들지 않아야 한다.

[표 2-4]에 나타난 MIPv6의 보안취약성은 대부분 서비스거부공격과 연관되어 있으며, 그 외에도 중간자 공격(Man-in-the-middle Attack), session hijacking, 위장 공격 등이 있다.

이러한 취약성들은 네트워크에서 이동성을 지원하기 위한 라우팅 기법들이 원인이 되므로 이에 대한 보안성을 제공해야 한다. 터널링 및 라우팅헤더를 이용시에 가질 수 있는 취약성은 유선망에서도 공통적이다. 그러나, 바인딩 업데이트와 홈어드레스 옵션(HAO) 사용시의 취약성은 이동 환경에서만 발생한다.

3) Mobility Support in IPv6 (RFC 3775), IETF

표 2-4 MIPv6의 보안취약성

구분	보안취약성
바인딩 업데이트	홈에이전트로의 바인딩 업데이트 메시지에 대한 취약성 CN과의 라우팅 최적화에 대한 취약성 MIPv6 CN의 기능이 다른 노드로의 반사 공격의 시발점으로 사용될 수 있는 취약성
홈어드레스 옵션	보안 기법들을 위한 고비용의 암호알고리즘들을 불필요하게 실행시키도록 하는 등의 공격을받을 수도 있음
라우팅헤더	MIPv6를 사용하는 IPv6 헤더가 침입차단시스템상의 규칙에 기반한 IP주소를 우회하거나다른 노드들로부터 트래픽을 반사시키는 데 사용될 취약성
터널링(IP헤더)	이동노드와 홈에이전트간의 터널에 이동노드가 트래픽을 보내는 것처럼 보이게 하는 공격으로 인한 취약성

MIPv6프로토콜에서는 이러한 보안취약점에 대응하고자, 단말의 핸드오프시 사용되는 메시지에 대한 대응 보안기술을 정의하고 있다. HA와 MN간은 사전에 SA를 맺고, IPSec의 전송모드로 BU메시지를 인증함으로써 BU메시지로 인한 보안취약성을 대응할 수 있다. 또한, CN과 MN 사이의 경로 최적화를 위하여 IPSec 터널모드의 RR(Return Routability) 기법으로 BU메시지에 대한 보안취약성에 대응한다.

자세한 보안취약성 및 이에 대한 대응방안은 아래와 같으며, MIPv6 노드를 인식하지 못하는 침입차단시스템의 주요 고려사항들은 다음과 같다.

1. 바인딩 업데이트

MN은 CN과 통신할 때 패킷의 소스 주소로 자신의 CoA를 사용하고 HAO에 자신의 HoA(Home Address)를 넣어서 전송한다. 이를 수신한 CN은 소스 주소와 HAO 내의 주소를 교체하여 사용한다. 이 때, 보안취약성을 이용한 위협요소로는 크게 보면 이동단말이 바인딩 업데이트 메시지를 HA로 전송할 때와 CN으로 전송할 때로 나눌 수 있다.

MN이 BU 메시지를 HA로 전송할 때, 공격자는 MN에 대해 현재 위치한 곳과 다른 곳에 위치해 있다는 정보를 줄 수 있고, HA가 이 정보를 받아들인다면, MN은 패킷을 받지 못하는 반면 다른 노드가 원하지 않는 패킷을 수신하게 된다.

또한, CN으로 BU 메시지를 전송할 때 공격자가 자신의 HoA를 희생자의 HoA로 설정하여 거짓 정보를 알릴 경우, CN에서 희생자로 전송하고자 하는 패킷은 공격자를 거치게 되므로 가용성과 기밀성을 모두 위협한다. 또한 공격자가 자신의 CoA를 거짓으로 알리는 경우, CN은 이동단말로 보내는 패킷을 모두 거짓 CoA로 전송하여 서비스 거부 공격을 할 수 있다.

그리고 CN으로 의미 없는 BU 메시지를 한꺼번에 많이 전송할 경우에는 CN에서 그 메시지가 유효하지 않음을 알아채기 전에 자원을 고갈시켜 의미 있는 패킷들을 처리할 수 없게 만든다.

마지막으로 공격자는 오래된 BU 메시지를 재실행하여 패킷들을 MN의 예전 위치로 전달시켜 MN이 패킷을 수신하지 못하게 만들 수 있다.

이를 위한 대응방안으로는 HA와 MN 사이에는 SA를 맺고, 교환되는 BU메시지에 대한 인증과정을 수행할 수 있다. 이를 위한 인증기법으로는 IPSec, RR과 CGA기법이 있으며 자세한 내용은 부록을 참조하길 바란다. BU인증 과정의 예로 MN이 BU 메시지를 전달할 때 HA로는 IPSec ESP를 사용하여 패킷을 보호하고, CN으로 BU 메시지를 전송할 때에는 RR을 이용하여 HoA와 CoA가 도달가능한지를 확인한 후 메시지를 전송하는 방식을 적용한다[4].

다음은 BU 메시지를 이용하여 임의의 위치, MN과의 동일 위치, HA와의 동일 위치, MN과 CN 사이의 위치, MN의 이전 위치 등으로 구분한 보안취약성과 그에 따른 대응방안이다.

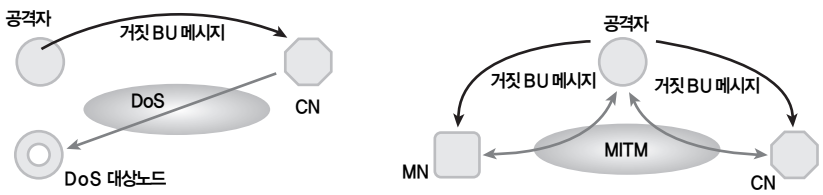
4) Using IPSec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents (RFC 3776), IETF

가. 임의의 위치에서의 보안취약성 및 대응방안

(1) 보안취약성

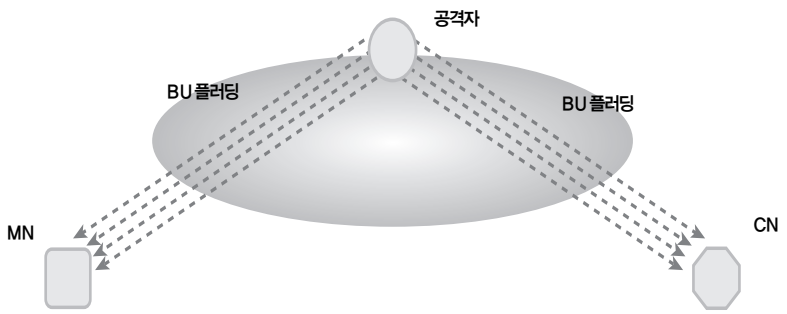
공격자는 MN의 HoA와 CN의 주소를 알고 있어 잘못된 CoA정보가 담긴 BU 메시지를 CN에게 보내어 해당 CoA를 가진 노드에게 서비스거부공격이 발생하도록 (그림 2-18)과 같이 유도할 수 있다. 또한 공격자가 BU 메시지를 MN과 CN에게 보내어 MN가 CN상에 교환되는 메시지를 중간에서 가로채거나 변조할 수 있다.

그림 2-18 임의의 위치에서의 보안취약성



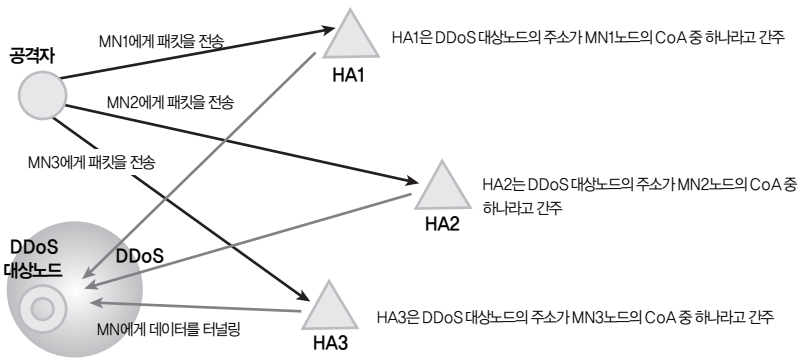
두 번째로 (그림 2-19)에서와 같이 CN으로 의미 없는 BU 메시지를 한꺼번에 많이 전송할 경우에 CN에서 그 메시지가 유효하지 않음을 알기 전에 CN의 자원을 고갈시켜 정상적인 패킷들을 처리할 수 없게 만든다.

그림 2-19 BU 메시지 플러딩을 이용한 보안취약성



세 번째로 공격자는 (그림 2-20)과 같이 잘못된 CoA를 가진 BU 메시지를 HA들에게 보냄으로써 HA는 MN의 잘못된 CoA 주소를 가지고 있도록 한다. 공격자는 각 MN의 HA에게 MN으로 보낼 메시지를 보내고 HA는 자신이 갖고 있는 MN의 CoA로 데이터를 터널링한다. 실제 CoA를 가진 노드에게는 분산 서비스거부공격을 초래할 수 있으며, 분산 서비스거부공격을 한 공격자는 자신을 숨길 수 있다.

그림 2-20 BU 메시지의 CoA 위조가 가능한 보안취약성



(2) 대응방안

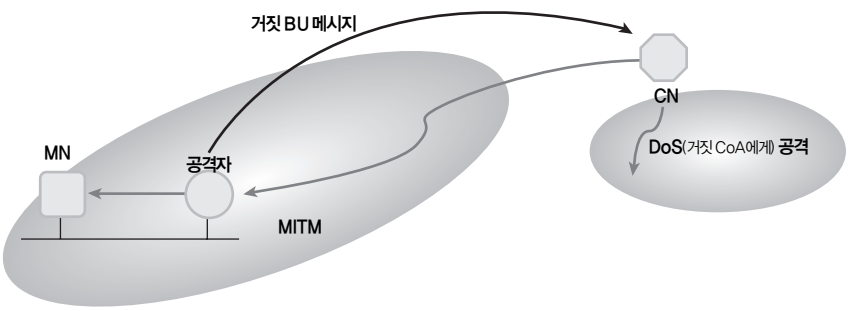
이러한 보안취약성에 대응하기 위해서는 첫 번째와 두 번째의 보안취약성의 경우, CN은 정상적인 MN으로부터 온 BU 메시지인지를 검증할 수 있어야 하며, BU 메시지를 거부할 수 있어야 한다. 또한, 세 번째 보안취약성에 대응하기 위해서는 MN과 HA간에는 SA가 있어야 하며 BU 메시지를 검증할 수 있어야 한다.

나. MN과의 동일 위치에서의 보안취약성 및 대응방안

(1) 보안취약성

(그림 2-21)에서와 같이 공격자는 MN과 같은 서브넷 상에서 MN의 BU 메시지를 관찰하여 CN에게 거짓 BU 메시지를 보낸다. 이를

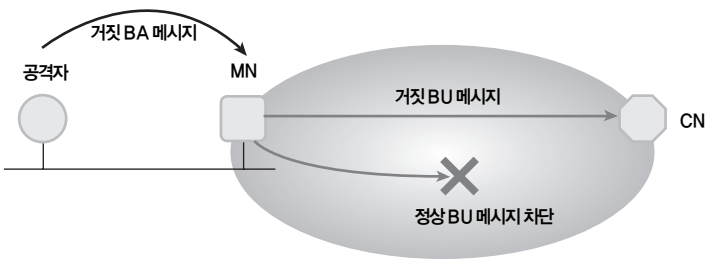
그림 2-21 허위 BU 메시지를 이용한 보안취약성



이용하여 공격자는 거짓 BU 메시지에 포함된 CoA주소로의 서비스 거부공격이 가능하다.

또 다른 보안취약성으로는 (그림 2-22)에서와 같이 공격자는 MN의 BU 메시지를 듣고 있다가 거짓 BA 메시지를 MN에게 보낸다. 이에 따라 MN은 불필요한 BU 메시지를 CN에게 보낼 수도 있고, 필요한 BU 메시지를 보내지 않을 수도 있다.

그림 2-22 허위 BA 메시지를 이용한 보안취약성



(2) 대응방안

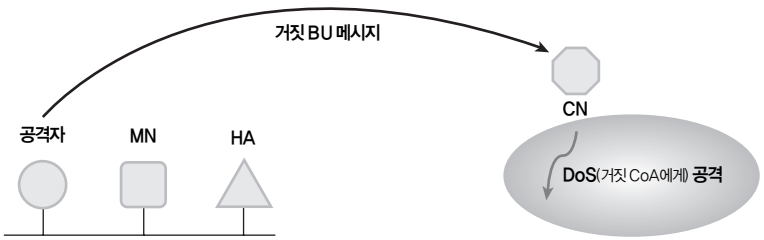
(그림 2-21)에 대한 대응방안으로는 CN은 BU 메시지의 송신자를 검증할 수 있어야 하며, (그림 2-22)의 경우는 MN이 BA 메시지의 송신자를 인증할 수 있어야 한다.

다. HA과의 동일 위치에서의 보안취약성 및 대응방안

(1) 보안취약성

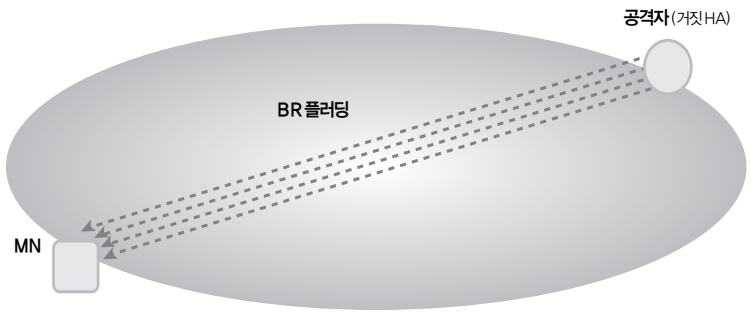
(그림 2-23)에서 MN이 HN에 있을 때, 공격자는 MN과 같은 서브넷에 존재하기 때문에 CN을 쉽게 알 수 있다. 이를 이용하여 공격자는 거짓의 BU 메시지를 CN에게 보낸다. 거짓의 BU 메시지에 포함된 CoA를 가진 실제 노드에게 서비스거부공격을 할 수 있다.

그림 2-23 BU 메시지의 CoA위조가 가능한 보안취약성



또한 공격자는 (그림 2-24)와 같이 MN으로부터의 BU 메시지를 스푸핑하여 HA로 위장하여 MN에게 BR 메시지를 보낸다. MN에게 BR 플러딩 공격을 가할 수 있다.

그림 2-24 BR 플러딩이 가능한 보안취약성



(2) 대응방안

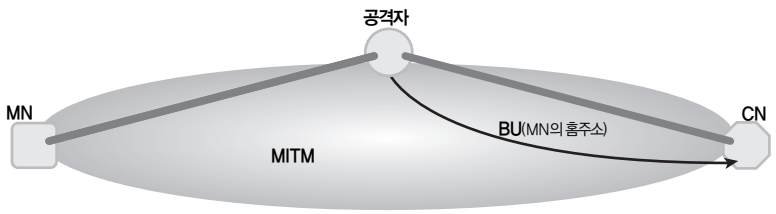
이에 대응하기 위해서는 MN이 BU 및 BR 메시지를 인증하여야만 한다.

라. MN과 CN사이에서의 보안취약성 및 대응방안

(1) 보안취약성

공격자는 MN의 HoA를 가진 BU 메시지를 CN에게 보냄으로써 (그림 2-25)와 같이 자신을 MN과 CN경로 상에 존재하게 하여 교환되는 데이터를 도청하거나 변조할 수 있다.

그림 2-25 위조된 BU 메시지를 이용한 보안취약성



(2) 대응방안

이는 CN이 BU 메시지를 보낸 송신자를 인증할 수 있어야 한다.

마. MN의 이전 위치에서의 보안취약성 및 대응방안

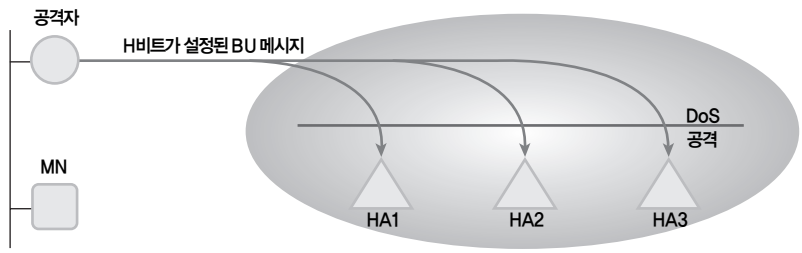
(1) 보안취약성

(그림 2-26)에서 공격자는 BU 메시지의 H비트를 설정하여 라우터에게 보냄으로써 MN에 대한 서비스거부공격이 가능하다. H비트는 MN이 자신의 홈에이전트를 찾을때 설정하는 비트로 홈링크상의 모든 라우터에게 H비트가 설정된 BU 메시지를 보낸다.

(2) 대응방안

HA가 BU 메시지를 보낸 송신자를 인증할 수 있어야 한다.

그림 2-26 BU 메시지 스푸핑이 가능한 보안취약성



2. 홈어드레스 옵션

MIPv6에서는 외부 네트워크에 위치한 MN이 CN에게 보낼 패킷의 소스 주소에는 CoA, HAO 필드에는 HoA를 표시하며, CN에서의 MIP 계층에서 CoA와 HoA를 교환하여 소스 주소가 HoA인 것처럼 만들고, IP 이상의 계층에서는 MN의 현재 위치에 무관하게 통신이 수행되도록 한다.

가. 보안취약성

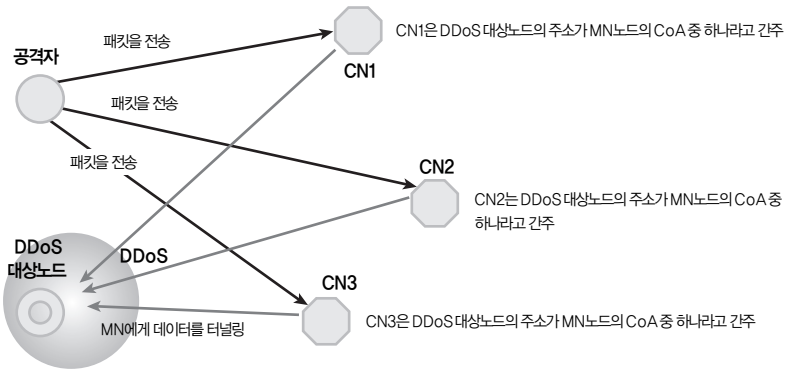
HAO를 사용할 경우 발생할 수 있는 보안상의 취약성은 공격자가 HAO를 사용하여 서비스거부공격을 할 수 있다는 것이다. 공격자는 (그림 2-27)에서와 같이 전송 패킷의 HAO필드에 공격대상 주소를 넣어 전송하면 CN은 그 주소로 응답한다. 즉, CN을 이용하여 공격대상 노드에 서비스 거부 공격을 할 수 있다.

또한 암호화 통신을 수행하는 환경에서는 공격대상 노드들이 전송된 암호화 패킷을 복호화하기 위한 작업을 수행하게 하여 계산 부하를 갖게 한다.

나. 대응방안

위와 같은 보안취약성은 CN이 수신한 패킷의 소스주소가 유효한

그림 2-27 HAO를 이용한 보안취약성



바인딩 주소인지를 검증함으로써 방지할 수 있다. 현재 RR기법을 이용하여 BU에 관련된 메시지를 검증함으로써 HAO의 보안취약성을 해결하고 있다.

그 외의 방안들을 살펴보면, 첫 번째 방안으로 인프라기반의 인그레스 필터링(infrastructure-based ingress filtering)기법을 사용하는 것이다. 이 방법은 AAA(Authentication, Authorization and Accounting)와 같은 글로벌 인프라를 이용한 지능적인 인그레스 필터링을 수행하도록 하는 것이다.

두 번째 방안은 인프라가 없는 인그레스 필터링(infrastructure-less ingress filtering)기법을 사용하는 것으로 주소에 대한 소유권을 보장할 수 있는 방법이다. MN은 CN으로 소스주소가 HoA인 메시지를 전송하면 이 메시지를 라우터에서 가로채어 이동단말로 AR(Authentication Request) 메시지를 전송한다. MN은 이 AR 메시지에 대해서 주소 소유권을 보장하기 위해서 라우터를 CN과 같다고 가정하고 RR이나 CGA 방법을 사용한 후, 메시지를 재전송하게 된다. 그러나 라우터에서 추가적인 프로세싱이 요구되므로 이에 따른 지연이 발생할 수 있으며, 구조적으로 종단간 방식과 네트워크 중심 방식 중에서 선택해야 하며 두 방식 모두 확장하기 어렵고 전개가 늦어질 수 있다.

세 번째 방안은 CN에서 HAO를 갖고 있는 패킷을 수신했을 때, 바인딩 정보 혹은 IPSec SA가 존재하는 경우에만 HAO 처리하도록 제한하는 것이다. 이 방식은 종단간 속성을 갖고 있으며 망에서 지원해야 할 별도의 기능이 필요 없다. 그러나 현재 MIPv6 규격에서는 바인딩 캐시 엔트리가 삭제되면 응답 패킷을 HA를 거쳐서 라우팅 되도록 지원하는 반면 이 방식에서는, 종료된 바인딩 캐시 엔트리에 해당하는 HAO를 가진 패킷을 수신할 경우 패킷을 버린다. 이 문제를 해결할 수 있는 방법으로 바인딩 캐시 엔트리와 일치하지 않는 HAO에 대해서 ICMP 에러 메시지를 생성하여 패킷 소스로 전송함으로써, HAO로 인한 추가적인 보안취약성의 발생을 막을 수 있다.

네 번째 방안은 반사된 패킷에 추가적인 정보로 패킷을 생성하는 소스 주소 갖도록 처리하는 것이다. 이를 위해 HAO에 대응하는 목적지 옵션을 정의하여 이용하는 방법이 가능하며 이를 위해서 MIPv6 표준규격을 수정하는 것은 어렵지 않다. 하지만 이 방식은 예방이 아니라 추적을 위한 것으로서 예방이 가능하게 하려면 침입차단시스템에 추가적인 기능을 구현해야 하고, HAO를 포함하는 패킷을 수신하였을 때, 이에 대응하는 옵션을 포함한 응답을 전송하도록 하거나 UDP 응용을 위해서 IPv6 소켓 API를 수정해야 할 필요가 있다.

3. 라우팅 헤더

라우팅 헤더는 상위계층 간의 투명한 통신을 위해서 MIPv6 환경에서 CN이 MN으로 패킷을 전송할 때 사용된다. 또한, multihoming 환경에서 라우팅 헤더의 소스 라우팅을 이용하여 동적으로 ISP를 선택할 수 있다.

가. 보안취약성

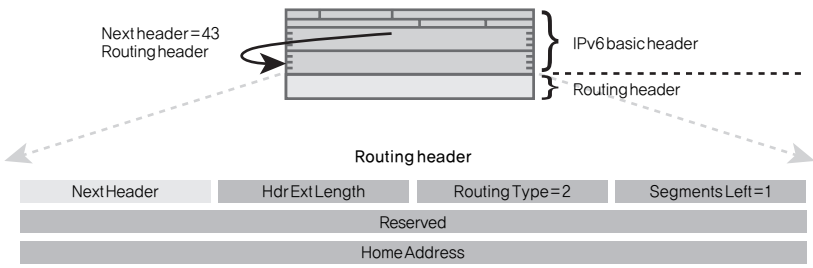
기존의 MIPv6에서 사용하도록 한 Type 0의 라우팅 헤더는 호스트나 라우터에서 모두 처리 가능하며, 여러 개의 주소를 담아서 전송

될 수 있기 때문에 반사 공격(reflection attack)에 이용될 수 있다.

나. 대응방안

MIPv6에 기존의 라우팅 헤더를 사용하지 않고 새로운 목적지 옵션, 새로운 확장 헤더 또는 새로운 라우팅 헤더 타입을 정의하여 사용하는 것으로 이를 위해 (그림 2-28)과 같이 Type 2의 라우팅 헤더가 새로이 정의되어서 보안 취약성에 대응하고 있다.

그림 2-28 Type 2 라우팅 헤더



그 외에 대응방안은 라우팅 헤더 자체를 안전하게 사용하는 것이다. 즉, 호스트나 내부 라우터들은 라우팅 헤더를 처리하여 전송할 수 없도록 하는 것이다. 이 방법은 모든 호스트와 라우터에서 라우팅 헤더를 처리하여 전송하는 것을 제한하기 때문에 초기에 의도한 라우팅 헤더의 목적으로 사용할 수 없고, MIPv6에서만 유용하게 사용되는 단점이 있다.

그리고 침입차단시스템의 기능을 강화하는 것으로 이 방법은 침입차단시스템에서 MIPv6를 지원하기 위한 규칙을 사용하는 것이다. 이는 침입차단시스템의 규칙이 복잡해지고 강화된 필터링으로 인해서 경로 최적화에 실패하는 경우도 발생할 수 있는 문제점이 있다.

4. 터널링

가. 보안취약성

HA와 MN간 터널의 부적절한 사용은 보안취약성이 될 수 있다. 만약 알 수 없는 노드가 터널링된 패킷 내부헤더상의 희생자 노드 MN의 목적지주소 부분에는 거짓주소를 포함하여 HA에게 보낸다면 HA는 해당 패킷을 MN에게 전달한다. 이 또한 서비스거부공격에 사용될 수 있으며 수신한 노드들에게 불필요한 보안 알고리즘을 수행하여 많은 컴퓨터자원을 소모시킬 수 있다.

나. 대응방안

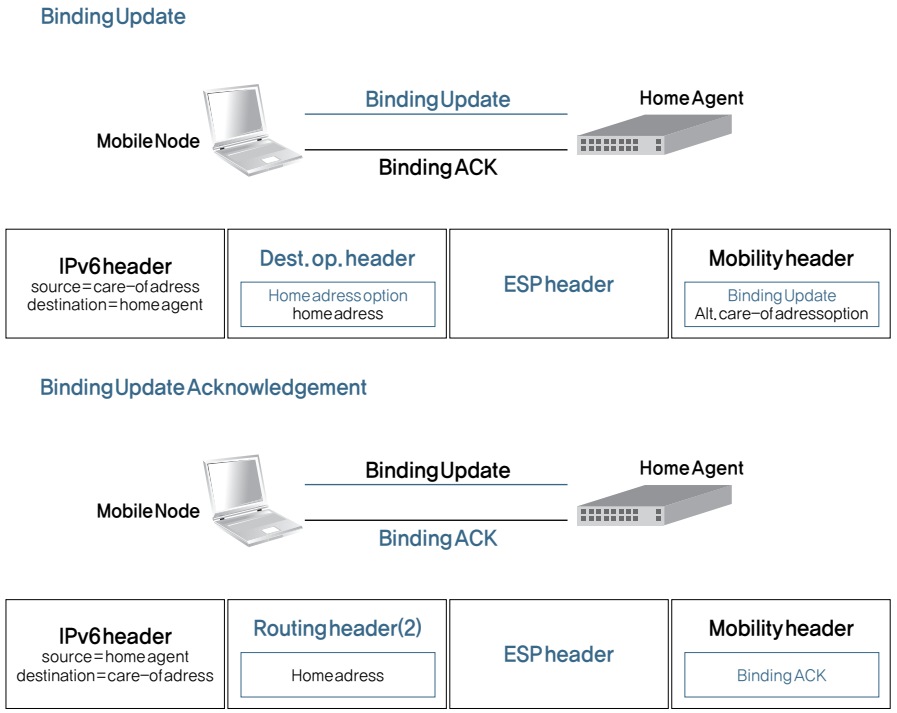
HA가 패킷을 전달하기 전에 수신한 터널링된 패킷의 내부 및 외부 IP헤더상의 소스 주소들이 유효한 바인딩인지 검증함으로써 이를 방지할 수 있다.

5. MIPv6 프로토콜에서의 대응기술

가. MIPv6 표준 보안 기술

MIPv6 표준에서는 이러한 보안취약성에 대응하기 위하여 메시지들의 인증절차를 정의하고 있다. HA와 MN간에는 사전에 SA(Security Association)이 맺어져야 하며, 이를 기반으로 하여 IPSec(IP Security)의 Transport모드로 ESP(Encapsulation Security Payload)헤더를 이용하여 BU, BA(Bingding update Acknowledgement) 및 BR(Binding update Request) 메시지 인증을 수행한다. 또한, MN과 CN사이에는 사전에 SA를 맺기가 어렵기 때문에, RR(Return Routability) 기법을 적용하여 BU, BA 및 BR 메시지의 인증을 통해 바인딩 업데이트 및 HAO 옵션의 취약점을 해결할 수 있다. (그림 2-29)는 HA와 MN이 바인딩 업데이트를 위해 교환하는 메시지들의 헤더부분을 나타낸 것으로 바인딩 업데이트(Binding Upadate)메시지의 헤더 부분에서 목적지 옵션 헤더

그림 2-29 HA와 MN사이의 바인딩 업데이트 메시지 인증

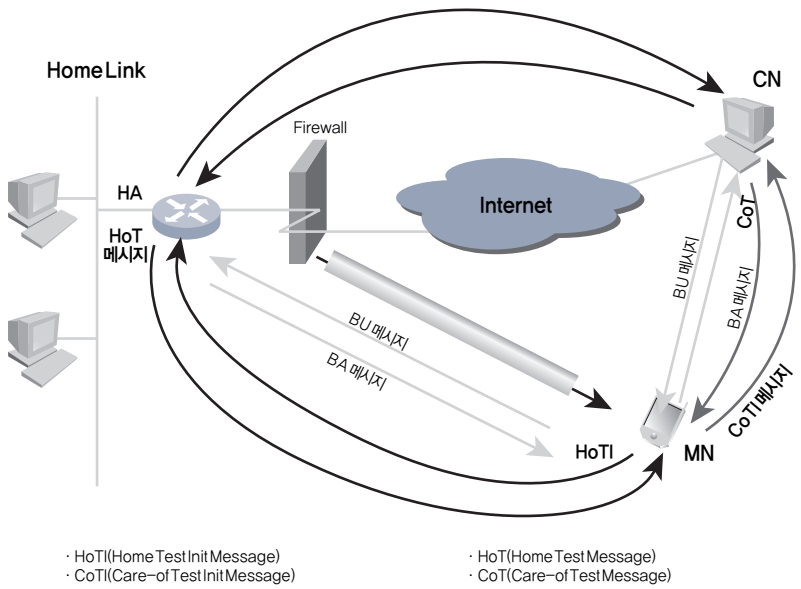


(Destination Option Header)에 포함되는 "Home address"는 미리 협약된 SA를 확인하는데 사용되며, ESP Header를 붙여서 MN BU메시지를 수신시 검증할 수 있도록 한다. 또한 BA메시지의 헤더 부분에서 라우팅 헤더(Routing Header)에 "Home address"를 넣는 것은 SA를 확인하기 위해서이며, "Binding Ack"부분은 암호화되고 , ESP헤더를 붙임으로서 이를 수신한 HA가 메시지를 검증할 수 있도록 하였다. 여기서 라우팅 헤더는 소스 라우팅에서 사용되는 것과 구별하여 소스 라우팅으로 인한 보안취약점을 방지하기 위해 라우팅 헤더를 사용하지 못하도록 할 경우에도 MIPv6가 정상동적을 할 수 있도록 type 2로 정의하여 사용된다.

(그림 2-30)은 MN과 CN사이의 바인딩 업데이트 메시지들의 인증을 위해 사용되는 RR절차를 나타낸 것이다. 먼저 MN이 쿠키정보를 담은 HoTI메시지를 HA를 경유하여 CN에게 보내고, CoTI를 CN

에게 보낸다. 이를 수신한 CN은 임의로 생성한 키를 이용하여 HMAC_SHA1 알고리즘에 홈주소, HoA 넌스 정보 등을 입력으로 한 출력값의 처음 64비트만을 잘라내어 Home Keygen Token을 생성하고, 마찬가지 방법으로 CoA와 CoA Nonce정보 등을 입력으로 하여 Care-of Key Token를 생성하여 MN에게 각각 HoT 및 CoT메시지에 실어서 보내준다. CN는 이후 두 토큰 정보를 이용하여 인증에 사용될 킷값을 생성하며, 이 두메시지를 수신한 MN 또한 이를 이용하여 메시지 인증에 사용될 킷값을 유도한다. 이후, MN은 인증키를 이용하여 BU메시지의 인증정보를 생성하고 이와 함께 BU를 CN에게 보내고, CN은 마찬가지로 인증정보화 함께 BA를 보냄으로써 검증된 바인딩 업데이트 메시지들의 교환이 이루어지도록 한다. 이를 이용하여 BU 메시지의 위변조를 통한 보안위협에는 대응할 수 있도록 하였다. 그러나 IPv6 주소 자체의 검증은 불가능하므로 부록에 간략히 설명하고 있는 CGA(Cryptographically Generated Address)기법을 이용하여 이에 대한 검증이 가능할 것이다.

그림 2-30 MN과 CN사이에서의 RR 동작 개요



BA메시지의 라우팅 헤더의 사용으로 인한 보안위협에 대응하기 위해서는 MIPv6에 기존의 라우팅 헤더를 사용하지 말고 새로운 목적지 옵션, 새로운 확장 헤더 또는 새로운 라우팅 헤더 타입을 정의하여 사용하는 것으로 이를 위해 Type 2의 라우팅 헤더가 새로이 정의되어서 보안 취약성에 대응한다. 그 외에 대응방안은 라우팅 헤더 자체를 안전하게 사용하는 것이다. 즉, 호스트나 내부 라우터들은 라우팅 헤더를 처리하여 전송할 수 없도록 하는 것이다. 이 방법은 모든 호스트와 라우터에서 라우팅 헤더를 처리하여 전송하는 것을 제한하기 때문에 초기에 의도한 라우팅 헤더의 목적으로 사용할 수 없고, MIPv6에서만 유용하게 사용되는 단점이 있다.

나. MIPv6 보안기술에서의 고려사항

바인딩 관련 메시지를 인증함으로써 대부분의 보안취약성을 보완하고 있지만, 기술을 지원하기 위한 추가 보안고려사항이 존재한다.

MN은 HA를 찾아서 자신의 HA를 선택하기 위해 ICMP Home Agent Address Discovery Request/Reply를 단말이 속한 네트워크상의 임의의 HA와 교환하게 되는데, 이때 공격자가 이 Request 메시지를 보냄으로써 HA의 위치를 알아낼 수 있어 네트워크의 관리 영역이 노출될 위험이 있다. 이를 위해서는 HA는 MN에게 응답메시지를 보낼대, MN로부터 온 요청 메세지가 정당한 것인지를 검증할 수 있어야 한다.

또한 MIPv6 보안 표준 기술에서 HA와 SA가 맺어져야 한다고 하였으나, SA를 수행하기 위한 과정은 정의되지 않았다. 최근 MIPv6를 표준화 중인 IETF에서는 모바일 단말이 HA를 검색하고 선택하는 과정에서 HA와 MN간의 SA기법에 대한 논의가 이루어지고 있다. 한 가지는 HA와 MN간에 IKEv2를 이용하여 직접 수행하여 SA를 맺는 것이며 다른 한 가지는 3GPP와 같은 이동통신에서 사용하는 기법으로 AAA등을 이용하여 신뢰적인 제 3의 보안서버를 이용하여 SA를 수행할 수 있다. 덧붙여서, DNS시스템을 이용하여 HA를 선택하여, HA-MN간의 인증을 통하여 SA를 수행할 수 있는 방안도 고려되고 있다.

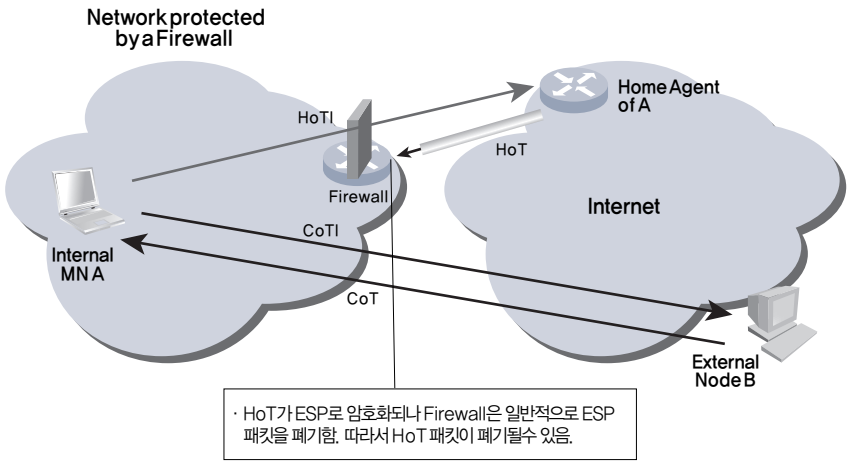
6. 침입차단시스템에서의 고려사항

MN, HA 또는 CN 중 한 개의 노드가 침입차단시스템에 의해 보호되는 내부 네트워크에 위치하는 환경에서, 침입차단시스템에 의해 MN을 위한 바인딩 업데이트, BU메시지에 대한 검증, 일반 패킷전송 까지도 차단될 수 있다. 따라서 시나리오 별로 침입차단시스템에서 고려해야 하는 사항은 다음과 같다.

가. MN이 침입차단시스템이 보호하는 네트워크 안에 존재할 경우

(그림 2-31)와 같이 MN이 침입차단시스템이 보호하는 네트워크 안에 있을 경우를 고려해보자.

그림 2-31 MN이 침입차단시스템이 보호하는 네트워크 안에 있을 경우



(1) MN A가 네트워크에 연결될 때, 로컬 IP 주소(CoA)를 확보해야 한다. 따라서 MN A는 현재의 상태 정보 업데이트를 위해 HA에 BU 메시지를 전송한다. BU와 BA 메시지는 MIPv6 규격에 의해 IPSec ESP로 암호화되어야 한다. 하지만, 기본적으로 침입차단시스템은 ESP 패킷을 폐기하므로, BU와 BA 메시지가 폐기될 가능성이 있다.

(2) CN B가 MN A와 통신을 하고자 할 때, CN B는 MN A의 HoA로 패킷을 전송한다. 전송된 패킷은 MN의 HA가 수신 후 MN의 CoA 주소로 터널링하여 전송한다. 이 때 침입차단시스템은 상태 정보가 업데이트 되어있지 않다면, 그 패킷을 폐기하므로 CN B는 MN A와 통신할 수 없다. 또한, HA가 MN A의 바인딩 정보를 업데이트할지라도 침입차단시스템은 CN B가 MN A와 통신하는 것을 차단할 수 있다.

(3) MN A가 Route Optimization(RO)를 사용한다면, HA를 거치지 않고 직접 CN B와 통신이 가능하다. 하지만, 침입차단시스템에서 RO 수행에 필요한 RR 절차에서 사용되는 메시지들이 차단될 수 있다.

(4) MN A가 HA에 바인딩 업데이트를 전송한 후 HA는 MN A의 CoA로 응답한다. 그러나 침입차단시스템은 MN A의 바인딩 정보가 없기 때문에 그러한 패킷들을 폐기할 수 있다. 따라서 침입차단시스템은 MN A의 CoA를 기반으로 MN A의 바인딩 정보를 업데이트해야 한다.

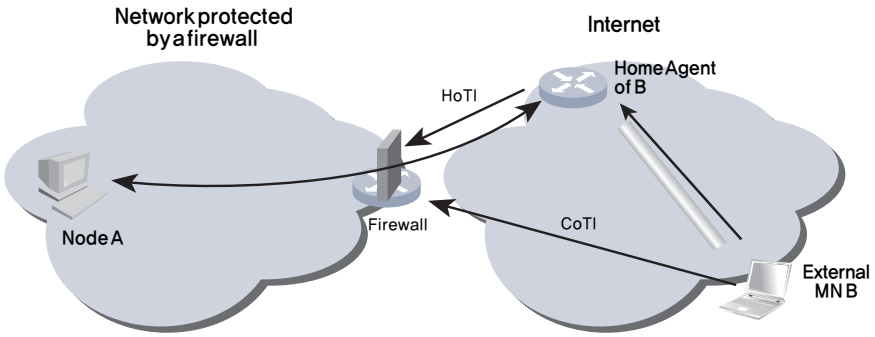
(5) MN A가 다른 침입차단시스템이 보호하는 네트워크로 이동하는 경우를 고려할 수 있다. MN A가 CN B에 BU 메시지를 전송할지라도 새로운 침입차단시스템은 MN A에 대한 바인딩 정보가 없기 때문에 BU 메시지를 폐기하게 된다.

나. CN이 침입차단시스템이 보호하는 네트워크 안에 존재할 경우

(그림 2-32)과 같이 MN B가 침입차단시스템이 보호하는 네트워크 안에 있을 경우에는 다음과 같이 RO와 관련된 취약성을 고려해야 한다.

MN B에 대한 바인딩 업데이트가 CN A에서 수행된 환경에서 침입차단시스템은 MN B에 대한 바인딩 정보로 HoA를 가지므로 소스 주소가 CoA인 패킷들과 CN A에서 MN B의 CoA로 전송되는 패킷을 폐기한다. 따라서 침입차단시스템은 MN B의 바인딩 정보로 CoA 정보를 추가적으로 업데이트해야 한다. 외부에서 내부 CN A로 전송된 BU 메시지에 대해 침입차단시스템이 검증을 지원하지 않으므로

그림 2-32 CN이 침입차단시스템이 보호하는 네트워크 안에 있을 경우



서비스거부공격이 발생할 수 있다. 즉, 공격자는 악의적인 BU 메시지를 전송하여 침입차단시스템으로 하여금 강제적으로 바인딩 정보를 변경시켜 정상적인 패킷까지도 폐기하게 할 수 있다.

다. HA가 침입차단시스템이 보호하는 네트워크 안에 존재할 경우

HA가 침입차단시스템이 보호하는 네트워크 안에 있을 경우에는 다음과 같은 사항을 고려해야 한다.

(1) BU 메시지, HoT 메시지 등과 같은 MIPv6 메시지들은 IPSec ESP로 암호화되어 전송되기 때문에, 침입차단시스템이 ESP 트래픽을 인식하지 못한다면, 이러한 MIPv6 메시지들은 폐기될 것이다.

(2) HA를 보호하는 침입차단시스템이 내부의 HA로 향하는 트래픽을 차단한다면, CN에서 HA로 전송되는 연결 설정 요청 메시지와 MN에서 HA로 전송되는 패킷들을 폐기할 수 있다.

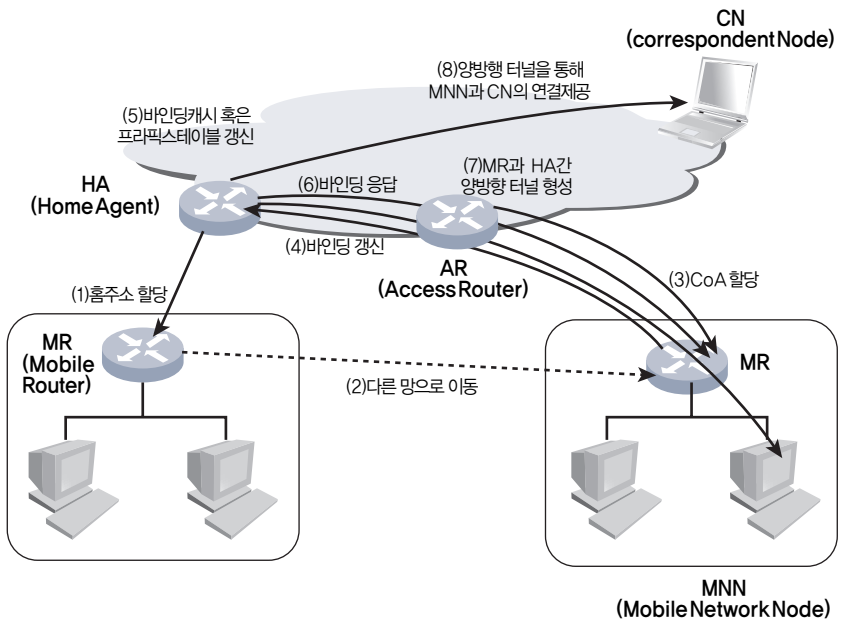
(3) HA가 다수의 침입차단시스템이 보호하는 하나의 네트워크 내에 있다면, 다수의 침입차단시스템 중 트래픽에 관련된 바인딩 정보를 가지고 있지 않는 침입차단시스템은 그 메시지를 폐기할 수 있다.

따라서, 위와 같은 경우가 발생하지 않도록 침입차단시스템에 이동 노드를 위한 필터링 규칙을 추가해야 한다.

이동 네트워크는 Mobile IP의 호스트의 이동성 지원의 확장된 개념으로 다수의 호스트가 이루는 네트워크 전체가 이동하는 형태이다. 이러한 이동 네트워크의 예로는 많은 호스트들을 가지고 있는 기차 비행기 선박 등이 있으며 승객들이 소지한 핸드폰, PDA, 노트북 등은 이동 라우터에 접속된 호스트가 된다.

네트워크 이동성 지원은 네트워크 자체가 이동하면서도 이동 네트워크 내의 각 호스트들에 대해 투명한 이동성을 제공하는 것을 목표로 한다. 즉 이동 네트워크내의 각 호스트들은 이동성 지원 프로토콜의 지원을 받지 않고 주소의 변화 없이 투명하고 안전하게 이동성을 제공 받아야 한다.

그림 2-33 NEMO 기본 동작 흐름도



(그림 2-33)은 NEMO(NEwork MObility)의 기본 동작 과정을 나타낸 것이다. 이동 라우터는 홈 망에서 IPv6 주소, 즉 홈 주소를 할당 받으며, 다른 망으로 이동한 경우 그 망으로부터 또 하나의 주소 CoA(Care of Address)를 할당 받아 이동 라우터가 현재의 위치를 알릴 수 있는 방법으로 사용한다. 그러나 이동 라우터가 어느 위치에 존재하든지 홈 주소에 의해 식별되며, 이동망 내의 단말들 또한 항상 홈 주소를 이용하여 통신하게 된다. 이와 같이 이동라우터는 홈 주소 및 CoA를 자동 할당 받을 때, DHCP(Dynamic Host Configuration Protocol) 서버로부터 할당 받거나, 인접 라우터의 RA(Router Advertisement) 메시지의 프리픽스 정보를 이용하여 자동으로 구성할 수 있다.

이러한 네트워크 이동성에 대한 잠재적인 보안 위협은 MR과 HA 사이의 IPsec 터널과 IP-in-IP 터널을 기본적으로 사용하는 이동 네트워크의 기본 동작으로 인해 발생할 수 있으며, 터널 패킷은 잘못된 소스 주소 또는 목적지 주소로 변경될 위협을 가지고 있다.

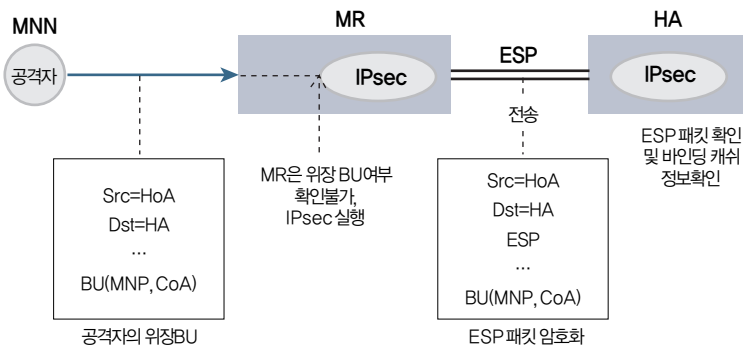
1. MR-HA IPsec Transport SA에 대한 위협

가. BU 스푸핑

(그림 2-34)를 살펴보면 MR에 내부로 인입되는 패킷에 대한 필터링이 제공되지 않는 경우에 발생하게 되는 경우의 공격 시나리오를 나타낸 것이다.

(그림 2-34)에서 공격자 MNN(Mobile Network Node)은 소스 주소에 MR(Mobile Router)의 HoA를 넣고 목적지 주소에 HA주소를 넣고 페이로드로 MR의 BU를 포함하게 세팅하여 스푸핑 패킷을 생성한다. BU 메시지의 포맷과 내용은 정상적인 MR로부터의 BU 메시지로 보여지게 된다. MR이 공격자로부터 이 패킷을 수신하게 되면, 먼저 버퍼에 저장하고 패킷의 SPD(security payload

그림 2-34 MNN 공격자의 BU 스푸핑



database)를 검사하게 된다. 이러한 경우 MR은 위조 패킷여부를 알 수 없으며 IPsec 처리가 필요한 패킷을 보안 인터페이스에 전달한다. IPsec 모듈은 ESP(Encapsulating Security Payload) 전송 모드와 소스노드의 주소를 사용하여 패킷을 캡슐화 한다.

HA가 이러한 패킷을 수신하면 IPsec ESP 소스노드 주소를 검사하여 패킷의 유효성을 검증한다. 최종적으로 HA는 MR로부터 BU가 전송된 것으로 오인하게 되고 바인딩 캐쉬를 수정하게 된다.

나. 대응방안

BU/BA 보호를 위해 기본적으로 BU를 보내기에 앞서 BU를 보호하기 위한 키 또는 SA를 확립하는 절차를 두고, MN과 MR 사이에 확립된 공유 비밀키를 사용하여 BU를 보호해야 한다. 또한 DNS로 공격자의 접근이 성공하더라도 다른 응용 서비스의 노출을 제한할 수 있어야 한다. 이를 위해 DNS의 보안적 확장 개념인 DNSSEC 기술을 새로운 대응 방안으로 마련하고 있다. 이러한 기법을 통해 송신자 인증, 데이터 무결성, 재전송 방지 및 기밀성을 제공할 수 있다.

2. MR-HA IP-in-IP 터널에 대한 위협

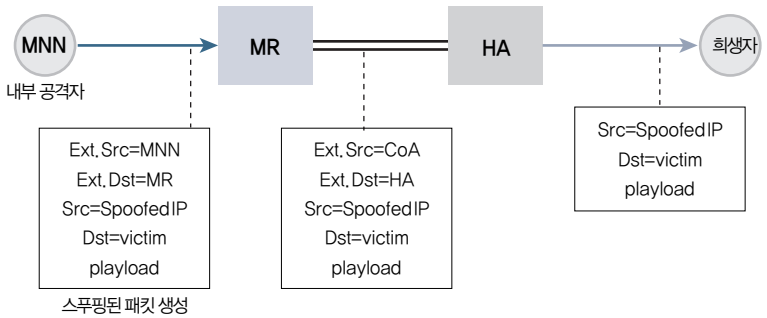
MR에서 IP-in-IP 터널패킷을 처리하는 경우 특정 목적용의 프로토콜 번호를 갖는 암호화와 복호화 모듈을 요구한다. 보안 IP-in-IP 터널 패킷들은 IPsec 터널 모드 암호화 같은 특정 보안 메커니즘을 요구한다. IP-in-IP 터널 패킷에 대한 공격은 이동 네트워크의 내부로부터 MR로 시작되거나 외부에서 직접적으로 HA로 가능하다.

가. 내부로부터의 공격

공격자는 (그림 2-35)와 같이 이동 네트워크 내부의 또다른 MNN 주소를 외부 소스 주소로 설정하고 외부 목적지 주소를 MR의 주소로 설정하여 조작된 IP-in-IP 패킷을 생성한다. 암호화된 패킷 내부의 내부 소스 주소는 스푸핑된 IP주소로 설정하고 내부 목적지 주소는 공격 목표물의 주소로 설정한다.

MR이 이 패킷을 수신하면 복호화 과정을 수행하고 IP-in-IP 암호화된 패킷을 HA에 전달한다. 즉, MR은 IP-in-IP 포맷(외부 소스 주소 = MR의 CoA, 외부 목적지 주소=HA 주소)으로 내부 페이로드를 암호화 하고 HA로 패킷을 전송한다. HA는 이러한 패킷을 수

그림 2-35 내부에서의 공격 시나리오

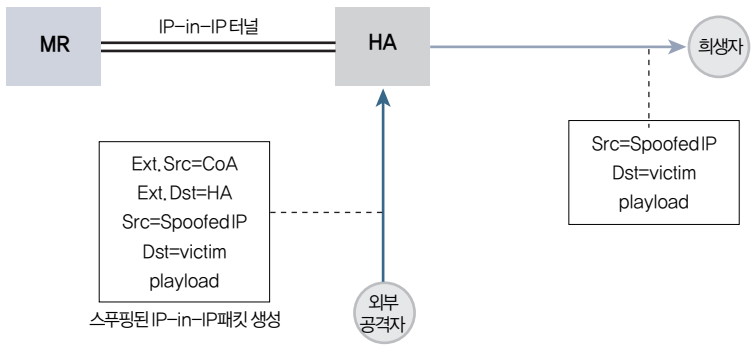


신한 후 공격목표물에 전송하게 된다. 이러한 절차를 통해 공격 목표물에 대하여 IP 스푸핑 또는 DoS 공격을 수행할 수 있다.

나. 외부로부터의 공격

외부로부터 공격자는 외부 소스 주소를 MR의 CoA로 외부 목적지 주소를 HA의 주소로 설정하여 IP-in-IP 패킷을 조작할 수 있다. 또한 내부 소스 주소로 위조된 IP 주소와 내부 목적지 주소로 공격목표물 주소로 설정하게 한다.

그림 2-36 외부에서의 공격 시나리오



다. 대응방안

터널링된 전송 경로를 사용하는 패킷에 대하여 잘못된 소스 주소 또는 목적지 주소로 변경될 위협을 줄이기 위해서 HA, MN, MR사이에서 통신하는 중요한 제어 메시지 교환에 대해 보안성을 제공해야 한다.

내부로부터의 공격을 보호하기 위해 MR은 GRE(Generic Routing Encapsulation) 복호화 과정을 수행한 후 필터링 과정을

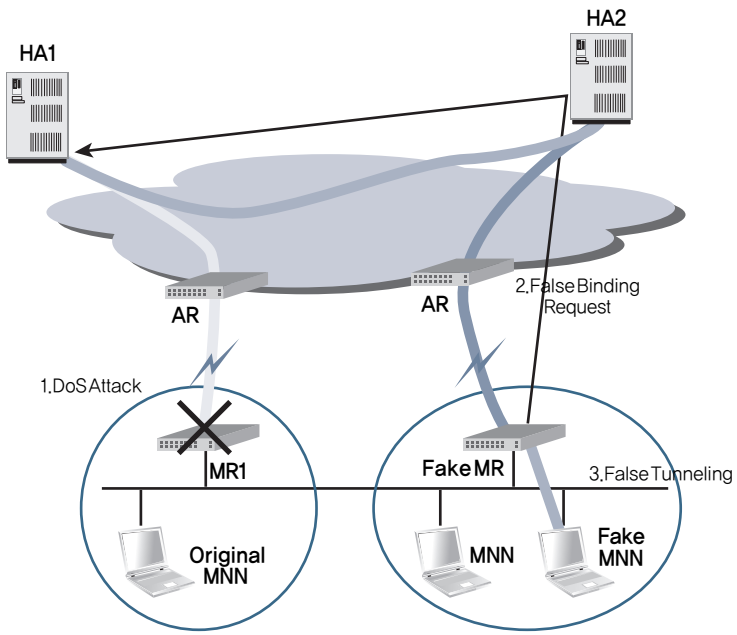
수행하여 조작된 패킷여부를 검사하는 과정을 통해 안전한 패킷만을 처리하도록 한다.

3. 멀티호밍 보안 위협

가. 리다이렉션 공격

일차적으로 리다이렉션 공격을 통해 프라이버시 정보가 외부에 유출되는 문제를 갖게 된다. 정상 MR을 DoS공격한 후 공격자가 위조된 MR정보를 이용하여 패킷을 수신할 수 있게 한다. 그리고 공격자는 패킷에 사용된 키 탐색을 위하여 도구를 사용할 수 있다. 결과적으로 탐색한 키를 이용하여 패킷을 조작하고 전송도 가능하다. 또한, 공격 목표물에 패킷을 대량으로 생성하여 전송하는 공격이 가능하다.

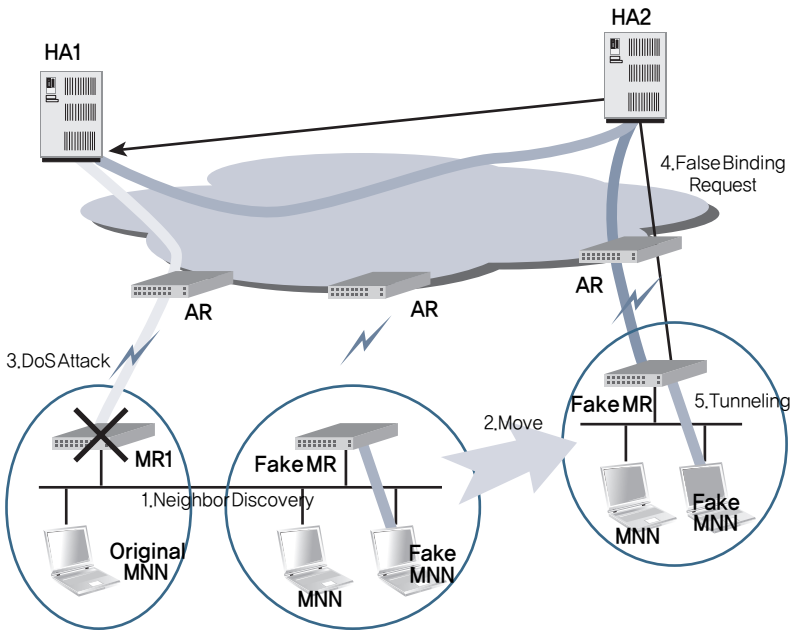
그림 2-37 리다이렉션 공격 시나리오



나. 재생 공격

조작된 MR이 이웃한 MR인 것처럼 위장하여 잘못된 CoA를 HA에 전송하여 False binding을 발생시킨다. 또한 프라이버시 침해, DoS공격, 리다이렉션 공격을 발생시킬 수 있다.

그림 2-38 재생 공격 시나리오



다. 대응방안

기본적으로 이동 라우터와 홈 에이전트간의 인증을 위해서는 사전에 보안 협약을 체결해야 하며, 홈 에이전트나 홈 네트워크 내에 보안 정책 데이터베이스를 구축하여 보안 협약 정보 및 보안 정책 정보의 유지, 관리가 이루어져야 한다.

세부적으로 리다이렉션 공격을 방지하기 위해서 이웃 MR들에 대하여 미리 인증된 경우에만 데이터의 처리를 허용하도록 하며, 재생 공격에 대응하기 위해서는 이웃 MR들에게 등록과 탈퇴의 과정을 수행시켜 적합한 MR인지의 여부를 결정하고 확인된 MR에 대해서만 데이터의 처리를 수행할 수 있어야 한다.

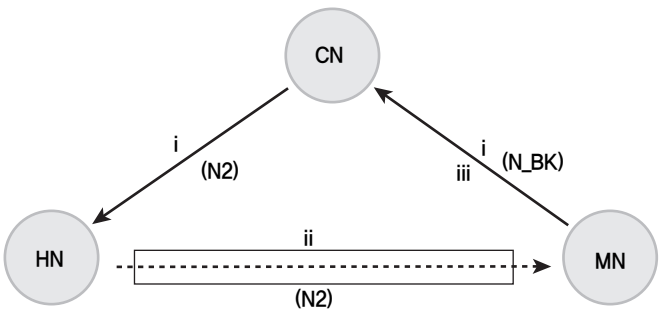
4. 이동성 네트워크 보안 대응기술

가. RR 방식의 BU 보안 기술

BU 보호를 위해 제안된 첫 번째 종류의 인증 메커니즘으로는 CN에서 HA를 경유하여 MN에게 보낸 패킷의 수신 여부를 확인하는 RR(Return Routability) 방식이다. 이것은 HA는 홈 등록을 통해 MN의 정확한 위치를 알고 있을 것으로 가정하여 MN에게 정확히 전달할 수 있을 것으로 기대하고 암호키 구성에 사용되는 값, 메시지의 인증 및 재전송 방지를 위한 비표(nonce)나 토큰 등을 보내며, MN으로부터의 응답을 통해 전송한 값이 제대로 전달되었는지 확인한다. 전달되는 메시지는 암호화되지 않는다.

RR 방식의 메커니즘 중의 하나인 BAKE(Binding Authentication Key Establishment)는 (그림 2-39)과 같은 3개의 메시지를

그림 2-39 BAKE 암호키 확립모델



이용하여 BU 인증에 사용될 암호키를 확립하는데, HA와 MN 사이에 보안을 위한 SA(Security Association)가 확립되어 있다고 가정한다.

(그림 2-39)에서 전달되는 메시지는 다음과 같다.

ⅰ. MN –〉 CN: 〈CoA, CNA, HoA, N1, T1〉
ⅱ. CN –〉 MN (HA 경유): 〈CNA, HoA, N1, T1, N2, T2〉
ⅲ. MN –〉 CN: 〈CoA, CNA, HoA, T0, T2, N_BK〉

표 2-5 기호 정의

기호	정의	기호	정의
CNA	CN의 주소	N1, N2, N_BK	난수
K_MN-HA	MN과 HA가 공유하는 비밀키	T0, T1, T2, N1	인증용 토큰
K_CN	CN만 알고있는 비밀키	BU	바인딩 갱신
BK	BU 보호에 사용하는 암호키	BR	바인딩 요청
BUR	HoA와 CoA를 포함하는 BU 요청메시지	BA	바인딩 확인

T0 = HMAC-SHA1-128 (K_MN-HA, N1 ‖ CNA ‖ CoA ‖ HoA)
T1 = SHA1-128 (T0 ‖ 32개의 공백문자)
T2 = HMAC-SHA1-128 (K_CN, T1 ‖ CoA ‖ CNA ‖ HoA)

Ti의 계산에서 "‖"는 연접을 나타내는 기호이며, SHA1-128은 해쉬 알고리즘 SHA-1을 적용한 결과에서 오른쪽 128비트만을 취하는 함수이며, HMAC-SHA1-128은 인증 알고리즘 HMAC-SHA1을 적용한 결과에서 오른쪽 128비트만을 취하는 함수이다.

메시지 ⅰ에서 보낸 T1이 메시지 ⅱ를 통해 HA에게 전달되면, HA는 T1의 사전 이미지 계산에서 K_MN-HA라는 MN과 HA가 공유하는 비밀키가 사용된 것을 확인할 수 있으며, 따라서 메시지 ⅰ의 송신자가 진정한 MN임이 확인된다. 메시지 ⅲ을 받게 되는 CN은

자신이 HA를 통해 MN에게 전달한 메시지가 무사히 MN에게 전달된 것을 확인함으로써 HA가 인정하는 MN이 맞는 것으로 판단한다. 또한, 메시지 iii에 포함된 토큰 T0는 이 메시지를 보내는 MN이 메시지 i을 보낸 MN과 동일한 노드라는 사실을 확인시켜 준다. 이러한 프로토콜을 통해 CN은 HA가 그 정체를 보장하는 MN과 통신하고 있음을 확인할 수 있다. BU 보호에 사용될 암호키 BK(BU Key)는 해쉬 알고리즘 MD5를 사용하여 다음과 같이 계산된다.

BK = MD5 (N2 ‖ N_BK)

BK는 CN이 생성하여 HA를 경유하여 MN에게 보낸 N2와 MN이 생성하여 CN에게 직접 보낸 N_BK를 이용하여 계산된다. 이 값들은 암호화되지 않고 평문 상태로 전달되므로 제3자가 가로채어 BK를 계산할 수 있는데, 이를 위해서는 이 값들이 전달되는 두 개의 서로 다른 경로 모두에 접근할 수 있어야 한다.

BAKE가 BU 보호에 사용될 수 있는 암호키를 먼저 확립한 후 BU 메시지를 전달하는데 비해 BUSEC(BU Security)와 BU3WAY(BU three way)는 암호키 확립 없이 전송된 비표가 돌아오는지를 검사하는 방식으로 MN의 신분을 확인한다. 먼저 BUSEC에서 교환되는 메시지들은 다음과 같다.

① MN –〉 CN: 〈BU, Nm〉
② CN –〉 MN (HA 경유): 〈BR, Nc, Nm〉
③ MN –〉 CN: 〈BU, Nc, Nm〉
④ CN –〉 MN (HA 경유 않음) 〈BA, Nc, Nm〉

여기서 BU, BR, BA는 각각 바인딩 갱신, 바인딩 요청, 바인딩 확인을 나타내며, Nm과 Nc는 각각 MN과 CN이 생성한 난수이며 비표로 사용된다. MN과 CN은 각각 자신이 생성하여 보낸 비표가 다시 돌아오는 것으로 상대방이 통신 경로 상에 존재하는 노드임을 확인할 수 있다.

BU3WAY는 BUSEC이 4개의 메시지를 사용하는데 비해 3개의 메시지만을 사용하는데, 교환되는 메시지들은 다음과 같다.

(1) MN –〉 CN:	BUR(HoA, CoA)
(2) CN –〉 MN (HA 경유):	BUC(N1, 타임스탬프)
(3) MN –〉 CN:	BU(N1, 타임스탬프)

BUR은 HoA와 CoA를 포함하는 BU 요청이며, BUC는 N1과 타임스탬프를 포함하는 BU 시험이다. BU는 바인딩 갱신 메시지이다. N1은 CN만 알고 있는 비밀 정보를 사용하여 계산된 인증 토큰이다.

N1 = hash(secret, HoA, CoA, CNA, 타임스탬프, 유효 기간)

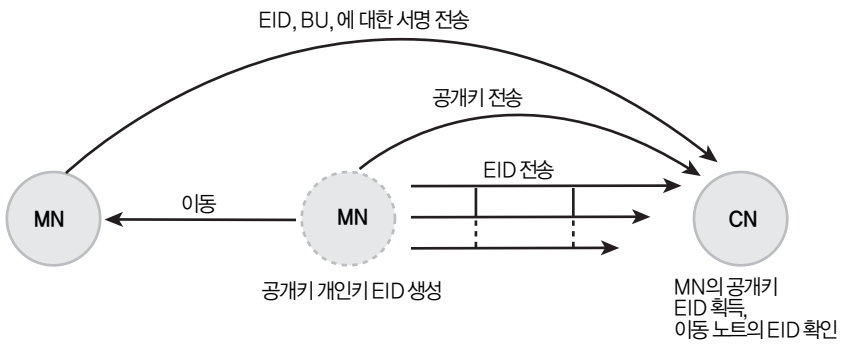
N1과 타임스탬프를 사용함으로써 CN은 메시지 (2)를 보낸 후 아무런 상태도 저장할 필요가 없으며, 따라서 BU 관련 메모리 소모가 원인이 되는 서비스 거부 공격을 방지할 수 있다. RR 방식의 메커니즘들은 다른 메커니즘들이 높은 비용의 공개키 연산을 사용하는데 비해 난수 생성이나 해쉬 함수 정도의 암호 기술만을 사용함으로써 계산 비용 측면에서 가장 효율적이라 할 수 있다.

나. 공개키 관련 ID 방식의 BU 보안 기술

두 번째 유형의 BU 보안 메커니즘에서는 BU 보호를 위해 공개키 서명을 사용한다. 가장 먼저 발표된 PBK(Purpose Built Keys)에서는 서명에 사용될 임시 공개키/개인키 쌍을 먼저 생성하는데, 일반적인 공개키가 일정 기간 동안 반복해서 사용되는데 비해, PBK는 임시키를 특별한 목적을 위해 한 번만 사용한다. 공개키 부분에 대한 해쉬 결과를 EID(Endpoint ID)라고 부르며, MN이 현재의 접속지에서 CN과의 세션이 시작될 때 여러 번 EID를 보내고, 현재의 접속지에 있는 동안 적절한 시점에 해당 공개키도 CN에게 보내둔다. MN이 다음 접속지로 이동한 후 〈EID, BU, (개인키로) BU에 대한 서명〉 등을 보내면, CN은 EID에 해당하는 공개키를 사용하여 서명을 확인할 수 있으며, 따라서 BU 메시지를 보낸 노드가 이전에 EID를 보냈

던 그 노드임을 확인한다. PBK는 BU 메시지를 보낸 노드의 유효성을 확인할 수 없지만, 이전에 HoA라는 홈 어드레스를 갖는 것으로 알고 있던 노드에서 메시지가 왔다고 믿게 하는 것이 그 원리이다. 또한 EID를 여러 번 보냄으로써 EID의 손실이나 EID 조작 공격에 대응할 수 있다.

그림 2-40 ID 방식의 BU 보안 메커니즘



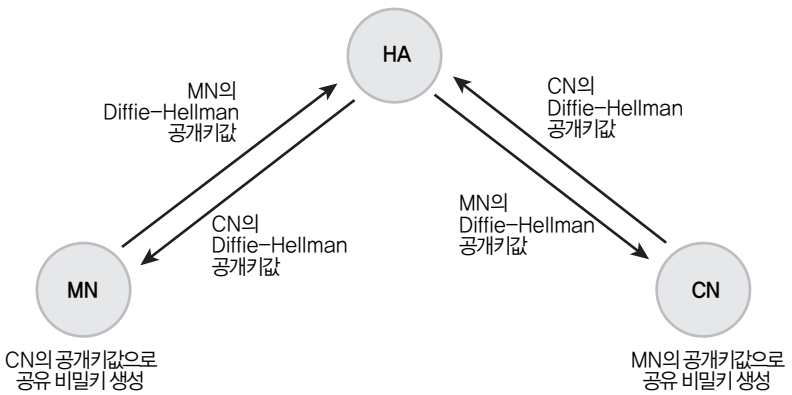
SUCV(Statistic Uniqueness and Cryptographic Verifiability)에서는 MN이 갖는 공개키 해쉬 값의 64비트를 MN의 HoA와 CoA 모두에 대해 IPv6 주소의 마지막 64비트로 사용한다. 이것은 PBK의 EID 전달 방식에 비교할 때, MN이 해당 공개키의 소유주임을 MN과의 모든 메시지 교환에서 확인할 수 있다는 점과 또 그 값이 주소에 포함되어 있어 별도의 대역폭을 차지하지 않는다. SUCV는 BU 보호를 위한 비밀키는 Diffie-Hellman 키 교환 방식을 사용해서 생성하고, CN이 Diffie-Hellman 키 교환 상대에 대한 인증을 위해 MN이 만들어 보낸 공개키 서명을 확인하는 방식을 사용하며, CN이 MN에게 보내는 Diffie-Hellman 공개 값은 HA를 경유하게 함으로써 부분적인 경로 검증까지 사용한다. 그리고, BU 보호는 IPsec ESP(Encapsulating Security Payload) 방식을 사용한다.

CAM-DH(Child-proof Authentication for MIPv6 with Diffie-Hellman)에서는 공개키 해쉬 값의 64비트를 MN의 HoA의 마지막 64비트로 사용한다. CoA의 경우에는 외지 네트워크에서 주소를 얻는 프로토콜에 따라 MN에게 주소 선택권이 없는 네트워크 환경도 존재하기 때문에 공개키 해쉬 값을 주소 구성에 사용하지 않는다. CAM-DH는 Diffie-Hellman 키 교환 방식을 사용하는 점에 있어서는 SUCV와 유사하지만, Diffie-Hellman 키 교환 메시지의 인증을 위해 MN의 개인키에 의한 서명도 사용하고 또 CN이 MN에게 HA 경유 여부에 따라 달라지는 두 개의 서로 다른 경로를 통해 전달한 값을 이용하여 생성된 키를 이용한 인증도 사용함으로써 좀 더 철저한 경로 검증을 거친다.

다. Diffie-Hellman 키 교환 방식의 BU 보안 기술

세 번째 유형의 BU 보안 메커니즘에서는 BU 보호를 위해 Diffie-Hellman 키 교환 방식을 통해 확립된 암호키를 사용한다. DHMIPv6(Diffie-Hellman based key distribution for MIPv6)에서는 MN과 CN이 각각 Diffie-Hellman 공개 값을 상대방에게 전달하는데, MN에게 보내는 메시지는 HA를 경유하여 전달된다. 이 방식은

그림 2-41 DHMIPv6의 보안 메커니즘



공개키 서명과 공개키 해쉬 값을 이용한 MN의 주소 지정 등을 제외하면 SUCV와 유사하다. Diffie-Hellman 키 교환 방식에서도 중개인 공격이 가능하지만, 이를 위해서는 두 가지 전달 경로 모두에서 능동적 공격이 이루어져야 한다. DHMIPv6에서는 HA와 MN 사이에 사전 확립된 SA는 활용되지 않고, AAA(Authentication, Authorization, Accounting) 기반구조가 제공될 경우 이를 이용한 강한 인증 방식을 사용하도록 한다.

SAP(Security Association establishment Protocol for MIPv6)는 DHMIPv6와 유사하지만 HA 통신의 병목현상을 피하기 위해서 MN에게 보내는 메시지가 HA를 경유하지 않고 직접 전달되는 방식이 사용된다. Diffie-Hellman 키 교환 방식의 사용은 공개키 연산 시간이 좀 많이 걸리기는 하지만 능동적 공격 능력이 없는 공격자들로부터 효과적인 방어수단이라 할 수 있다.

제 3 장 IPv4/IPv6 전환기술의 보안취약성 및 대응방안

현재, IPv4 망에서 IPv6 망으로의 전환(Transition)기술로는 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation)이 있다. 본 장에서는 이러한 기술에 대하여 간략히 설명하고 보안취약성 및 대응방안을 알아본다.

제 1 절 IPv4/IPv6 듀얼스택

1. IPv4와 IPv6의 호환성 지원

IPv6 단말이 IPv4 단말과 호환성을 유지하는 가장 쉬운 방법은 IPv4/IPv6 듀얼 스택을 제공하는 것이다. (그림 3-1)은 듀얼 스택의 동작 개념도이다. IPv4 호스트는 듀얼 스택 호스트의 IPv4 계층을 이용하여 통신하고 IPv6 호스트는 IPv6 계층과 통신할 수 있다.

(그림 3-2)와 같이 IPv4/IPv6 듀얼 스택 노드는 양쪽 프로토콜을 모두 지원하기 때문에 IPv4 주소와 IPv6 주소로 모두 설정할 수 있다.

IPv4/IPv6 듀얼 스택 노드는 DHCP 등을 이용하여 해당 IPv4 주소를 얻고, 비상태형 자동 주소설정기법 등을 이용하여 IPv6 주소를 획득할 수 있다. 따라서 듀얼 스택 노드의 DNS는 도메인 네임과 IP 주소 간 매핑을 위해 IPv4와 IPv6 모두를 지원한다. 즉, IPv4의 A

그림 3-1 듀얼 스택의 동작 개념도

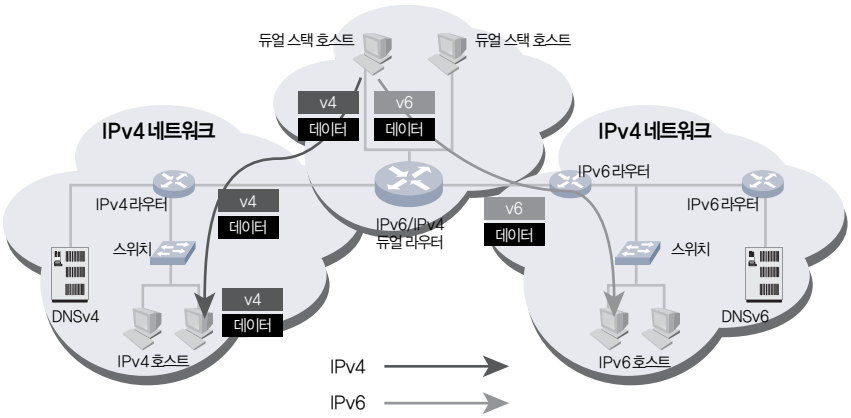
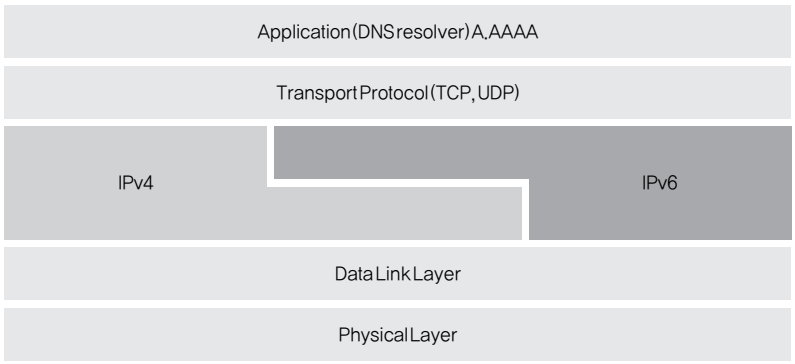


그림 3-2 듀얼 스택 구조



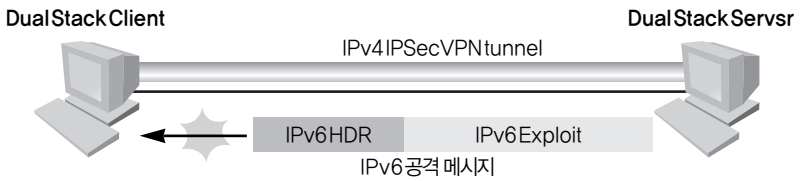
레코드는 물론이고, IPv6의 AAAA 레코드도 처리할 수 있다.

가. 보안취약성

듀얼스택 호스트에 대한 중요한 보안 고려사항은 IPv4에서 요구되는 보안수준이 IPv6 상에서도 동일하게 적용되어야 한다는 것이다. 따라서, IPv6/IPv4에 발생할 수 있는 모든 보안 취약성을 고려해야 한다. IPv4/IPv6 전환 시, (그림 3-3)과 같이 듀얼스택 클라이

언트가 IPv4에 대해서만 IPSecVPN을 지원하고, IPv6에 대해서 지원하지 않는다면 IPv6 패킷에 대한 안전한 통신을 보장하지 못한다.

그림 3-3 듀얼 스택의 보안취약성



나. 대응방안

이러한 보안취약성에 대응하기 위해서 호스트 침입방지시스템(Host Intrusion Prevention), 개인용 침입차단시스템(Personal Firewall), VPN 클라이언트(VPN Client)와 같은 장비가 IPv4, IPv6 두 가지 프로토콜을 모두 인식하여 트래픽을 검사하고 차단할 수 있어야 한다.

예를 들어, IPv4에서 설정된 침입차단시스템의 ACL(Access Control List)은 반드시 IPv6의 ACL에도 반영되어야 한다. IPv6 네트워크는 IPv4 네트워크와 토폴로지가 달라서 ACL의 일관성을 유지하기 어려울 수 있으나 IPv4와 동일한 보안 수준을 유지해야 한다.

일반적으로 터널링은 네트워크를 보호하기 위해 설치된 침입차단 시스템이나 침입탐지시스템을 우회할 수 있기 때문에 네트워크상에서 발생하는 보안 위협중의 하나이다.

터널링을 사용할 때 가장 먼저 MTU 설정과 관련된 취약성을 생각할 수 있다. 'ping'이나 'traceroute'같은 일반적인 네트워크 관리프로그램은 크기가 작은 패킷을 사용하기 때문에 MTU 사이즈를 잘못 설정해서 발생되는 오류를 탐지하기 어렵다.

MTU가 명시적으로 설정되지 않은 경우, 디폴트값이 사용된다. 예를 들어, CISCO의 IOS라면 디폴트 MTU값은 최종 단말을 향한 인터페이스에 의해 결정된다. 그러나 종단간의 MTU가 서로 다르게 설정되어 있다면, 전송받은 데이터를 인식하지 못 할 수도 있다.

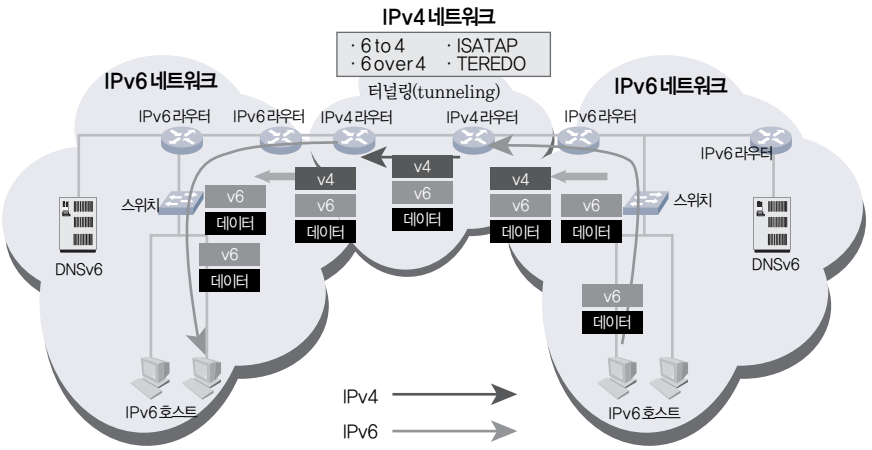
물론, 'path MTU discovery'를 사용하면 통신 경로상의 최대 MTU를 찾을 수 있다. 그러나 이것으로 터널의 종단간에 존재하는 단말노드의 MTU가 동일하다는 것을 보장할 수 없으므로 여전히 보안취약성은 존재한다.

1. IPv6-in-IPv4 터널링

가. 보안취약성

(그림 3-4)는 IPv6 데이터의 전송 경로에서 IPv4만을 인식하는 네트워크 구간에 대해 IPv6-in-IPv4 터널링을 적용한 예제이다. 터널링의 입구에서 IPv6 데이터는 IPv4 패킷에 캡슐화되어 전송된다. 이때 탑재된 데이터가 IPv6임을 표시하기 위해 IPv4 패킷 헤더의

그림 3-4 IPv6-in-IPv4 터널의 동작



프로토콜 필드 값을 41로 설정한다.

만약, 침입차단시스템이 IPv4 구간 내에만 위치하는 경우, IPv4 환경에 맞추어 운영되는 대다수의 침입차단시스템은 IPv6 패킷의 내용을 인식하지 못하므로 악의적인 IPv6 패킷을 차단할 수 없게 되는 보안취약성이 발생한다.

IPv6-in-IPv4 터널은 일단 설정 되고나면 마치 단대단 링크처럼 동작한다. 즉, IPv4 터널 내부의 네트워크 구성과는 무관하게 터널 전체가 하나의 hop처럼 동작한다. 만일 터널 내부의 어떤 링크에 문제가 발생한다면 관리자는 어떤 링크에 문제가 있는지 파악하기 어려울 수 있다.

터널 구간에서는 캡슐화를 위해 IPv4 헤더를 추가하므로, 터널 구간의 MTU는 path MTU보다 작아져 패킷 단편화가 발생할 수 있다.

나. 대응방안

IPv6-in-IPv4 터널링을 이용하여 IPv4 침입차단시스템을 우회하는 보안취약성을 해결하기 위해서는, 내부로 유입되는 IPv6 트래

픽을 적절하게 검사하고 필터링할 수 있는 IPv6 기반의 침입차단시스템을 터널 종단에 설치해야 한다. 또한, 침입차단시스템은 IPv6에 대한 사이트 경계에서 IPv4에 사용된 ACL 규칙을 IPv6용으로 변환하여 반영해야 한다.

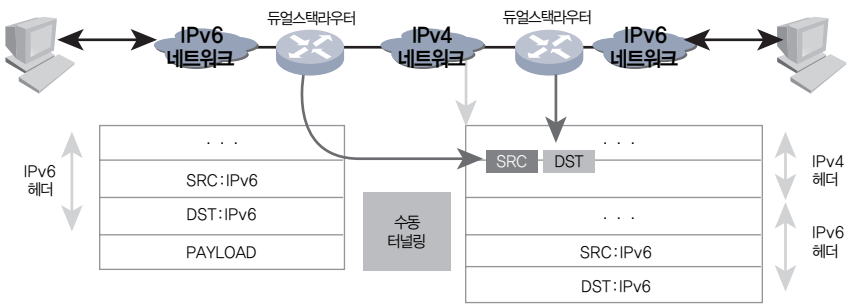
공격자가 ICMPv6 패킷을 이용하여 내부네트워크 호스트 주소에 대해 스푸핑 하는 것을 방지하기 위하여 인그레스(ingress) 필터링 뿐만 아니라 이그레스(egress) 필터링도 지원해야 한다.

IPv6-in-IPv4 터널 종단에서 디캡슐레이션된 IPv6 패킷은 글로벌 유니캐스트 주소를 가져야하므로 링크 로컬 주소를 갖는 패킷들은 침입차단시스템에서 폐기되어야 한다.

IPv6의 'path MTU discovery' 기능은 패킷 단편화의 보안취약성에 대한 대응방안이지만, 이 기능이 모든 터널에서 구현되어 있지 않으므로 IPv6-in-IPv4로 캡슐화된 패킷의 최소 MTU값인 1280바이트로만 전송한다면 IPv4의 최대 path MTU값이 1500바이트 이므로 패킷 분할의 문제를 방지할 수 있다.

IPv6-in-IPv4 터널링 방법은 크게 수동 터널링(configured tunneling) 방식과 자동 터널링(automatic tunneling) 방식으로 구분된다. 일반적으로 관리자가 네트워크 구간의 모든 부분을 파악하여 네트워크를 안정적으로 운영할 수 있다는 측면에서 수동 터널링

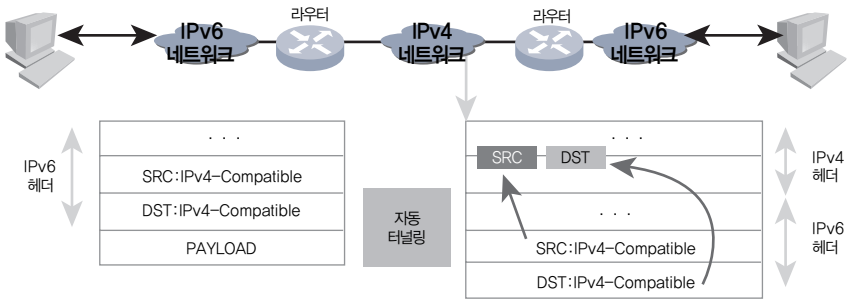
그림 3-5 수동 터널링의 동작



방식이 보안상 더 안전하다.

(그림 3-5)와 같이 수동 터널링은 6Bone에서 주로 사용하는 방법으로, 통신하는 두 장비 간에 고정된 IPv4 주소를 통해 정적으로 터널을 설정하는 방식이다.

그림 3-6 자동 터널링의 동작



반면에 (그림 3-6)과 같은 자동 터널링은 IPv4 호환 주소(IPv4-compatible address)를 이용해 수동 설정 없이, 패킷이 IPv4 구간을 통과할 때 IPv4 호환 주소에 내포돼 있는 IPv4 주소를 통해 자동으로 터널링을 설정하는 방식이다.

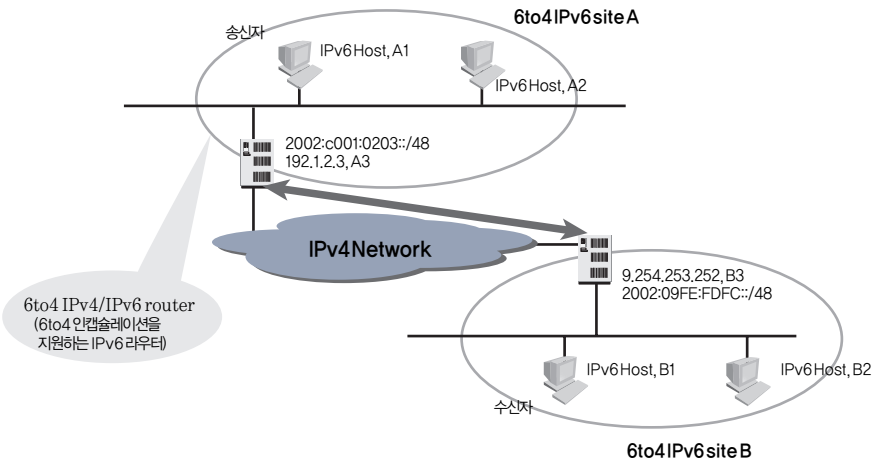
2. 6to4 터널링

가. 보안취약성

6to4는 듀얼스택을 갖는 호스트에 '2002:IPv4 주소::/48'의 단일 IPv6 프리픽스를 할당하여 자동 터널링을 통해 외부 IPv6 네트워크와 통신이 가능하도록 하며 (그림 3-7)과 같이 동작한다.

6to4 방식은 IPv6 주소에 IPv4 주소를 삽입하여 IPv4 망에서는 IPv4 패킷으로 라우팅 처리되고 IPv6 망에서는 IPv6 패킷으로 라우팅 처리되는 터널링 기술로 확장성이 뛰어나다.

그림 3-7 6to4의 동작



6to4에서 발생할 수 있는 주요한 보안취약성은 다음과 같다.

첫째, 터널링된 링크-로컬 패킷들이 6to4 가상 인터페이스를 원격 공격할 가능성이 있다. 만약 6to4 가상 인터페이스가 그 호스트의 다른 인터페이스로부터 분리되어 있지 않다면, 가상 인터페이스에 대한 원격공격은 모든 시스템에 영향을 미칠 수 있다.

둘째, 6to4 호스트들은 공격자가 조작한 IPv4-encapsulated IPv6 트래픽과 6to4 릴레이 서버로부터 수신한 트래픽을 구분하지 못한다. IPv6 노드에 대한 소스 주소 스푸핑과 RDoS(Reflection of Denial-of-Service) 공격 모두에 취약하다.

셋째, 공격자인 IPv6 노드가 자신의 실체를 숨기는 수단으로써 릴레이 서버를 이용할 수 있다. 즉, 공격자는 터널링된 패킷을 스푸핑하여 IPv4 호스트를 공격할 수 있다.

넷째, 6to4 릴레이 서버는 로컬 망에 대한 브로드캐스트 공격(broadcast attack)에 사용된다. 예를 들어, w.x.y.z/24의 주소로 설정된 릴레이가 있을 경우, 공격자는 w.x.y.255로 변경한 6to4 주

소로 설정된 패킷을 전송할 수 있다. 또한 “no ip directed broadcast”가 설정되어 있지 않다면, 원격에서도 이런 유형의 공격은 가능하다.

나. 대응방안

가상 인터페이스에 대해 아래와 같은 ACL을 추가함으로써 대응할 수 있다. (a)는 허용 가능한 주소범위를 지정하고, (b)는 (a) 이외의 주소 범위를 거부하는 예이다.

(a) allow from 2002::/16 to 2000::/3
(b) deny all

또한 관리자는 서로 다른 6to4 주소 간에는 릴레이하지 않도록 6to4 릴레이 서버를 설정해야 한다.

브로드캐스트 공격은 6to4 주소와 유사한 브로드캐스트 주소를 목적지 주소로 갖는 패킷에 대해 필터링하는 ACL을 설정하여 대응할 수 있다.

일반적으로 6to4 릴레이는 6to4 주소를 검증하여 보호할 수 있다. 즉, 6to4 주소내의 IPv4 주소가 글로벌 유니캐스트 주소이고, 실제 사용되는 IPv4 주소인지를 검증해야 한다.

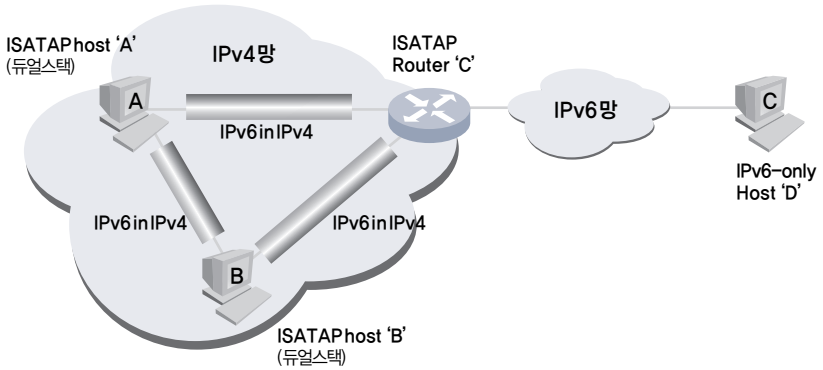
3. ISATAP(Intra Site Automatic Tunnel Address Protocol) 터널링

가. 보안취약성

ISATAP는 IPv4 네트워크 내부에 존재하는 듀얼스택 호스트가 IPv6 호스트와 통신을 하기위한 프로토콜로서 IPv4 터널링을 위한 별도의 라우터가 필요하다.

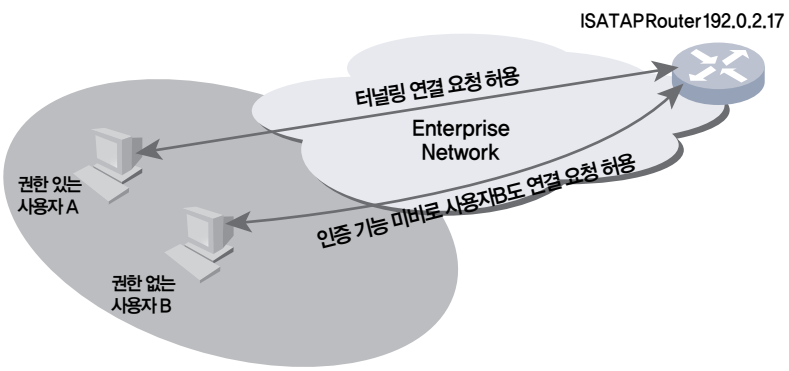
동작 과정은 (그림 3-8)과 같다. IPv4 네트워크 내의 듀얼스택 호스트 A가 IPv4 네트워크를 경유하여 IPv6 호스트 D와 통신하려고 한다면, A는 ISATAP 라우터 C에 IPv6 주소를 요청하여 자동으로 할당받는다. 이때 A에 의해 발송된 패킷은 C로 보내져 자동으로 캡슐화 되어 전송된다.

그림 3-8 ISATAP의 동작



ISATAP를 이용하면 IPv4 기반의 인트라넷 내부에 IPv6 네트워크를 설치할 수 있다. ISATAP를 이용하면 터널이 사용되므로, 캡슐

그림 3-9 사용자 인증 미비로 인한 ISATAP 보안취약성



화된 IPv6 패킷의 악성 여부를 판별하기 어렵다. 또한, (그림 3-9)와 같이 ISATAP 라우터의 사용자 인증기능이 약한 경우 공격자가 해당 ISATAP 라우터의 주소만 알아내면 터널을 사용할 수 있다.

나. 대응방안

사용자 인증이라는 측면에서 ISATAP 서버나 라우터는 내부 호스트들이 요청한 터널만을 정당한 것으로 인식하여야 한다. 이러한 접근제어는 침입차단시스템을 이용하면 간단하게 설정할 수 있다. 단, 침입차단시스템의 ACL을 설정할 때, IPv4 경계 라우터는 프로토콜 타입 41(IPv6-in -IPv4 트래픽)을 허용하도록 설정해야 한다.

또한, ISATAP 서버의 정보가 DHCP 등을 통해 외부로 유출되지 않도록 장비를 설정해야 하며, "Router Advertisement" 메시지나 "Neighbor Discovery" 메시지를 통한 정보 유출을 방지해야 한다.

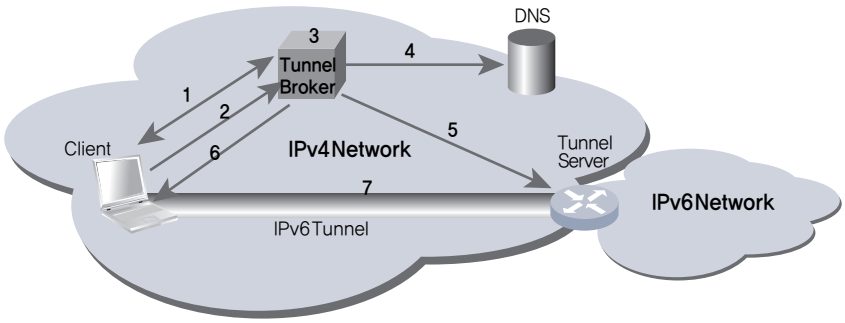
4. 터널 브로커(Tunnel Broker) 활용 터널링

가. 보안취약성

IPv6 네트워크에 안정적이고 지속적인 IPv6 주소와 도메인 네임을 전달하기 위해 도입된 개념으로서 터널 브로커라는 전용 서버를 구축하여 사용자의 터널링 요구를 자동으로 관리하는 방법이다. 현재 대부분의 6Bone 네트워크는 수동으로 설정된 터널을 사용하여 관리자의 작업이 많다. 그러나 터널 브로커는 자동 터널링 기법을 사용하여 기존 수동 터널의 단점인 터널 설정 및 관리상의 어려움을 해결할 수 있다.

(그림 3-10)의 동작 과정은 먼저 클라이언트와 터널 브로커 사이에 AAA를 통한 인증을 수행한다(1). 두번째로 터널 정보를 요청하고(2), 터널 브로커가 터널 서버, IPv6주소, 터널 유지 시간 등을 선택한다(3). 네번째는 DNS에 IPv6주소를 등록하고(4), 터널 설정 정보를 터널 서버에 전달한다(5). 또한 여섯번째로 클라이언트에게 터널

그림 3-10 터널브로커 동작



파라미터, DNS 명을 전달한다(6). 마지막으로 설정 정보를 통하여 클라이언트와 터널 서버 간에 터널링을 생성한다(7).

일부 터널 브로커 서비스는 사설 IPv4 환경에서도 IPv6 주소체계를 이용할 수 있는 NAT 기능을 지원하고, 터널 설정을 위한 프로토콜(TSP: Tunnel Setup Protocol)을 사용하는 전용 클라이언트를 제공하기도 한다.

그러나, 터널 브로커 사용자에 대한 적절한 인증 절차가 없다면, 보안취약점이 발생할 수 있다. 특히, 악의를 가진 공격자가 터널의 설정을 임의로 변경하면, 불법적으로 네트워크에 접근하거나 서비스 거부공격을 유발할 수 있다.

또한, 세션에 대한 관리가 부적절하다면, 공격자가 다른 사용자의 세션을 가로챌 수 있다. 이러한 보안취약성은 사용자별로 정적 IP 할당 서비스에서 보다 동적 IP 할당 서비스에서 발생하기 쉽다.

나. 대응방안

관리자는 터널 브로커 서비스를 사용하는 사용자에 대한 인증 메커니즘을 구축 · 운영 해야 한다. 인증의 방법에는 ID-패스워드 기반의 간단한 방법부터 KDC(Key Distribution Center) 등을 이용한

방법이 가능하다. RFC3129[5]에서는 사용자에게 Kerberos[6] 티켓을 발행하는 메커니즘이 제시되어 있다.

터널 양단의 네트워크 주소를 파악하여 패킷의 소스나 목적지 주소의 위조 여부를 판별하기 위해서 관리자는 터널에 대한 필터링 정책을 적용해야 한다. 예를 들어, A네트워크에서 터널을 경유하여 B네트워크로 전송되는 패킷의 목적지 주소가 A네트워크에서만 유효하다면 B네트워크에서 필터링해야 한다.

터널의 상태를 파악할 수 있는 모니터링 프로그램을 운영하는 것도 한 가지 대응방안이다. 즉, 터널의 트래픽을 모니터링하면 공격자가 악의적으로 패킷을 대량 전송하여 서비스를 마비시키려는 공격에 대응할 수 있다.

5. DSTM(Dual Stack Transition Mechanism) 터널링

가. 보안취약성

DSTM의 기능은 듀얼스택 호스트 상의 IPv4응용이 IPv4호스트와 통신을 필요로 하는 환경에서 IPv4-in-IPv6터널링을 제공하는 것이다.

DSTM 터널링을 구성하기 위해서는 [표 3-1]과 같은 세 가지 종류의 장비가 필요하다.

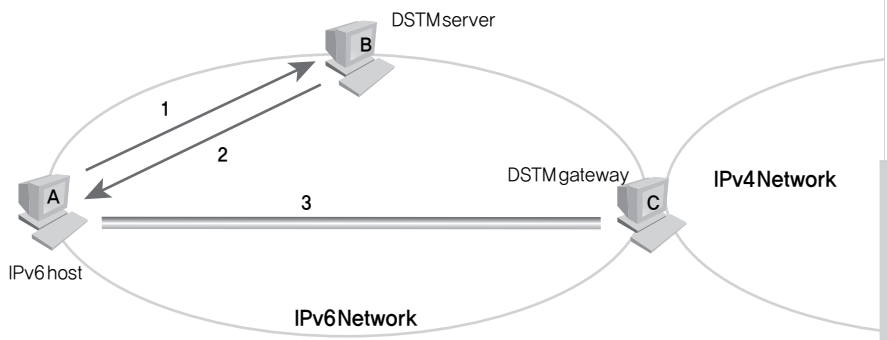
DSTM 구조에서는 DSTM 게이트웨이만이 항상 IPv4 네트워크에 접속되어 있으므로, 해당 게이트웨이만 IPv4 주소를 지속적으로 유지하면 된다. IPv4/IPv6 듀얼스택 호스트는 IPv4 네트워크와 통신을 원하는 경우에만 DSTM 서버에서 임시 IPv4 주소를 할당받아 사용하면 된다.

5) Requirements for Kerberized Internet Negotiation of Keys
6) 네트워크 사용자를 인증하는 것과 관련하여 미국 MIT의 아테네 프로젝트에서 개발된 네트워크 인증 표준

표 3-1 DSTM 터널링을 위한 구성요소

종류	장 비	동 작
A	**IPv4/IPv6 듀얼스택 호스트**	IPv6-only 네트워크 내부에 존재하지만 IPv4를 이용해 통신하기를 원함
B	**DSTM 서버**	IPv4 address pool을 유지하고 필요시 할당함
C	**DSTM 게이트웨이 (또는 TEP,Tunnel End-Point)**	IPv6 패킷에 IPv4캡슐화(encapsulation) 및 비캡슐화(decapsulation)를 수행

그림 3-11 DSTM 동작



DSTM 터널링 동작은 (그림 3-11)과 같다. 1, 2번 과정은 A가 B에게 임시 IPv4 주소를 요청하여 응답을 받는 과정으로 DHCPv6나 RPC를 통해 이루어질 수 있다. 응답 메시지에는 임시 IPv4 주소뿐만 아니라 해당 주소의 유효기간과 DSTM 게이트웨이 정보가 포함된다. A는 IPv4 프로토콜 스택을 설정하여 IPv4 네트워크로 향하는 IPv4 패킷은 IPv6 주소로 캡슐화되어 C까지 전송된다. C는 디캡슐화를 수행하기 위한 IPv4/IPv6 주소 맵핑 테이블을 유지한다.

DSTM에서는 공격자가 다른 호스트의 세션을 가로챌 수 있는 보안취약점이 있다. 예를 들어 (그림 3-11)의 A가 IPv4주소를 할당받아 IPv6 터널을 통해 IPv4 네트워크와 통신하는 경우, 공격자가 A의 IPv4 소스 주소를 도용하여 IPv4-in-IPv6 패킷을 보낸다면, C와 A 사이의 터널은 끊어지고, C와 공격자 사이의 터널로 교체된다.

나. 대응방안

현재까지는 DSTM 서비스 자체적으로 제공하는 인증기능이 미비하므로 관리자는 별도의 인증 메커니즘을 구축 · 운영해야 한다. 특히, DSTM 서버에서는 임시 IPv4 주소를 요구하는 호스트들에 대한 인증이 필요하다.

또한, 관리자는 현재 사용 중인 터널이 DSTM 서버에 의해 정상적으로 생성된 것인지를 항상 확인하고 비정상적인 트래픽을 차단하여야 한다.

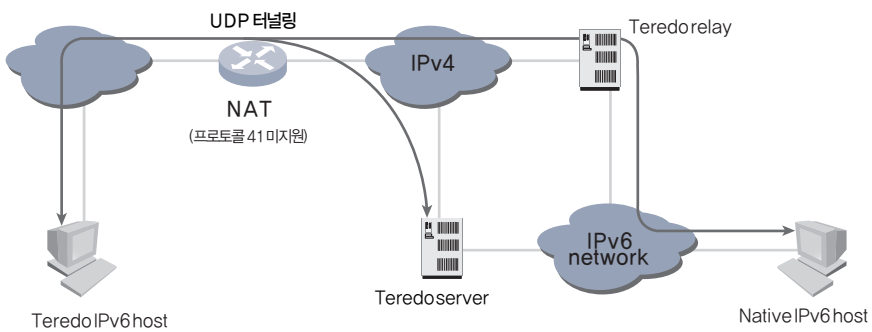
6. Teredo 터널링

가. 보안취약성

Teredo 터널링은 IPv6-in-IPv4 터널링 패킷을 지원하지 않는 IPv4용 NAT가 운용되는 환경에서 듀얼스택 노드에 UDP 상의 터널링 패킷을 통하여 IPv6 통신을 제공하는 기술이다.

(그림 3-12)는 Teredo IPv6 호스트가 UDP 터널링을 이용하여 Teredo 서버에게 터널링에 대한 요청을 보내고 IPv6 터널링 처리를 위한 릴레이를 통한 native IPv6 호스트와의 통신 과정을 보여주고 있다.

그림 3-12 Teredo동작



(1) NAT에서의 보안 취약성

NAT에서 Teredo관련 서비스를 허용하면서 침입차단시스템에서의 패킷 필터링 또한 허용시키는 경우에 허용된 서비스들을 이용한 공격이 가능하다.

(2) Teredo서비스를 이용한 보안취약성

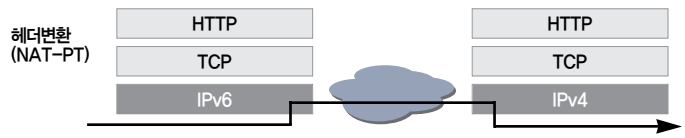
Teredo 서비스의 주목적은 NAT뒤에 위치한 호스트에게 글로벌 IPv6 주소를 제공하는 것이다. 이러한 환경에서 공격자는 RS를 가로채거나 스푸핑된 RA를 전송하거나 Teredo 클라이언트에게 잘못된 주소를 제공할 수 있다. 이러한 동작으로 클라이언트들의 통신에 대한 릴레이기능을 이용하여 중간자 공격을 할 수 있다. 또한 Teredo서버를 이용한 반사공격이 가능하다.

나. 대응방안

NAT 상에 생성된 보안 홀의 생성으로 인한 보안 취약성은 필요한 서비스에 대해서만 NAT에서 허용하고 IPv6용 개인 침입 차단 시스템 및 IKE, AH, ESP 같은 IPv6 보안 서비스를 사용하여 대응할 수 있다. 중간자 공격에 대한 대응방안으로는 클라이언트들이 외부로 IPv6패킷을 전송하는 경우, IPSec을 이용하여 무결성 및 기밀성을 제공하는 것이다.

본 절에서는 IPv4/IPv6 변환(translation)을 통해서 IPv4 호스트와 IPv6 호스트 사이에 통신 기술에 관한 보안취약성 및 대응방안을 기술한다. IPv4/IPv6 변환은 네트워크/전송/응용 계층에서 발생할 수 있고, 통신 호스트 간 트래픽 변환과 중계를 제공하는 서버를 필요로 하며, 변환을 수행하는 계층이 상위일수록 성능은 떨어진다. 본 안내서에서는 (그림 3-13)의 네트워크 계층 변환인 NAT-PT/NAPT-PT에 대한 보안취약성 및 대응방안을 기술한다.

그림 3-13 네트워크 계층 변환



1. NAT-PT/NAPT-PT(Network Address Translation-Protocol Translation /Network Address Port Translation-Protocol Translation)

가. 보안취약성

NAT-PT와 NAPT-PT는 IPv4 패킷을 IPv6 패킷으로 혹은 그 반대로 변환시켜 주는 기능을 한다. 단, NAT가 일대일로 IP 주소를 변환하는 것에 비해 NAPT는 다대일로 IP 주소를 변환시키고 포트 번호로 구분한다.

(1) 종단간 보안취약성

IPv6 호스트 A가 IPv4 호스트 B로 패킷을 송신할 때, 그 패킷은

IPv6 주소를 가지므로, IPv4로 변환해야 한다. 이때, IPv6에서 생성된 체크섬 등은 사용할 수 없게 된다. RFC2766[7]에도 NAT-PT를 사용하면 종단간 보안을 만족시킬 수 없음을 명시하고 있다.

(2) 프리픽스(prefix) 할당시 보안취약성

IPv6 호스트는 NAT-PT 장비로의 패킷 라우팅을 위한 프리픽스가 필요하다. 만약 프리픽스가 미리 설정되어 있다면 IPv4 호스트와의 통신에 필요한 IPv6 프리픽스를 사용할 수 있다. 그러나 NAT-PT 장비에 장애가 발생하여 서비스가 중단된 경우, 공격자가 IPv6 호스트에 조작된 IPv6 프리픽스를 할당하여, IPv4 호스트로 전달될 모든 패킷을 가로챌 수 있다.

(3) 소스주소 스푸핑 공격 가능성

NAT-PT 장비가 위치한 네트워크에서 공격자가 스푸핑된 패킷을 IPv4 네트워크로 다량 전송하면, 주소풀(Address Pool)의 IPv4 주소를 고갈시켜 서비스거부공격이 가능하다.

나. 대응방안

이러한 보안취약성에 대한 대응방안으로는 NAT-PT 에서 인그레스 필터링을 수행하는 것이다. 이것은 스터브(stub) 도메인에 있는 공격자가 소스 주소를 위조하지 못하게 하고, 동일한 도메인에 있는 다른 노드에 반사공격을 수행하지 못하게 한다.

IPv4 주소고갈 공격(Address Depletion Attack)은 IPv6 노드의 TCP/UDP 포트를 IPv4 노드의 주소에 부합하는 TCP/UDP 포트로 매핑을 지원하는 NAT-PT를 사용하여 방지할 수 있다.

NAT-PT 게이트웨이는 필터링을 통해 IPv4 소스 주소가 브로드캐스트/멀티캐스트 주소인 모든 패킷들을 폐기시키고, 서비스거부공격을 방지할 수 있다.

7) Network Address Translation – Protocol Translation (NAT-PT)

제 4 장 IPv4/IPv6 공통 보안취약성 및 대응방안

본 장에서는 IPv4 및 IPv6 네트워크 환경에서 공통적으로 나타날 수 있는 보안취약성을 이용하여 네트워크 계층에서 발생할 수 있는 스니핑 공격, 중간자 공격, 서비스 거부 공격에 대하여 설명하고 각각의 대응방안을 설명한다.

제 1 절 보안취약성

1. 스니핑 공격(Sniffing Attack)

스니핑 공격은 네트워크 상에서 데이터를 볼 수 있는 공격 형태로 Unix 운영체제에 포함된 Tcpdump 유틸리티 등을 악용하면 이러한 공격이 가능하다. 공격자는 스니핑 공격을 통해 다른 사용자의 로그인 정보를 보거나 평문 프로토콜을 이용하는 중요한 정보들을 훔쳐볼 수 있다. (그림 4-1)은 전형적인 스니핑 공격을 보여주고 있다.

2. 중간자 공격(Man-in-the-Middle Attack)

서버와 사용자간에 상호인증이 이루어지지 않으면 (그림 4-2)와 같은 중간자 공격(Man-in-the-Middle Attack)이 가능하다. 즉, 공격자는 송신자 측과는 수신자로 위장하며, 수신자 측과는 송신자로 위장하여 통신하고 있다. 중간자 공격은 IPSec에서의 ESP와 같은 보안 수단이 없는 경우 데이터 스트림의 불법 수정이나 거짓 데이터 스

그림 4-1 스니핑 공격

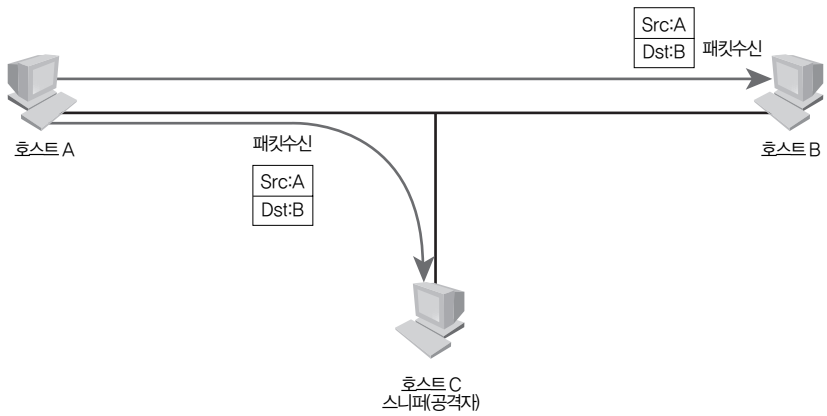
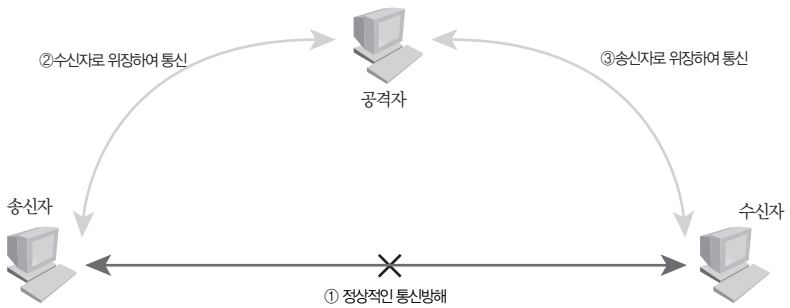


그림 4-2 중간자 공격



트림의 생성을 수반하며, 신분 위장(masquerade), 재전송(replay), 메시지 불법수정(modification of message), 그리고 서비스 거부 공격(denial of service)등의 적극적 형태의 공격이 가능하다.

3. 서비스 거부 공격(Denial of Service Attack)

IPv6에서 IP 주소의 범위가 늘어났지만 IPv4와 마찬가지로 플러딩 공격은 여전히 가능하다. 대표적인 공격으로는 SYN 플러딩(SYN

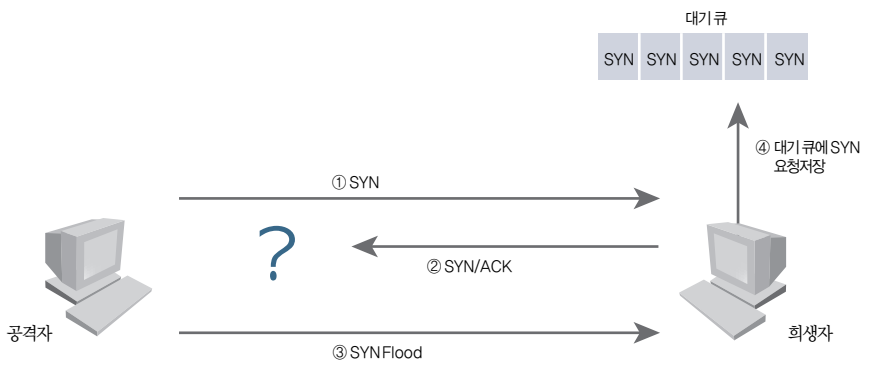
Flooding), UDP 플러딩(UDP Flooding), Smurf 공격(Smurf Attack), 분산 서비스 거부 공격(Distributed Denial of Service)등이 있다. 다량의 패킷이 발생되는 IP 소스의 필터링 및 QoS를 통한 대역폭 조절, 침입탐지시스템 등을 이용하면 일시적인 대응은 가능하나, 근본적으로 플러딩 공격에 대한 방어는 쉽지 않다. 분산 서비스거부공격이나 네트워크 장비에 대한 플러딩 공격을 통해 자원소모를 유발하는 문제 등은 IPv4나 IPv6에서 달라질 것이 없다.

가. SYN 플러딩(SYN Flooding)

서버에 접속을 요청하는 패킷을 보낸 후 정보를 보내지 않아 서버가 열린 상태로 기다리고 있는 경우 연결 설정이 초기화되기 전에 위조된 패킷을 플러딩하여 포트의 대기 큐(Backlog Queue)에 더 이상 저장할 수 없는 상태로 만드는 공격이다.

특정 시스템에 대한 불법적인 권한을 얻는 적극적인 방법이 아니라, 네트워크와 시스템의 자원을 공격 대상으로 하는 공격방법 중의 하나이다. 이것은 연결 지향적인 TCP를 이용한 공격이다. 즉, (그림 4-3)과 같이 SYN 플러딩은 TCP의 연결 과정인 Three-way handshaking을 이용하여 공격자가 희생자의 소스 IP 어드레스를 spoofing 하여 SYN 패킷을 특정 포트로 전송하게 되면 이 포트의 대기 큐를 가득 차게 하여 이 포트에 들어오는 연결요청을 큐가 빌 때까지 무시하도록 하는 방법이다.

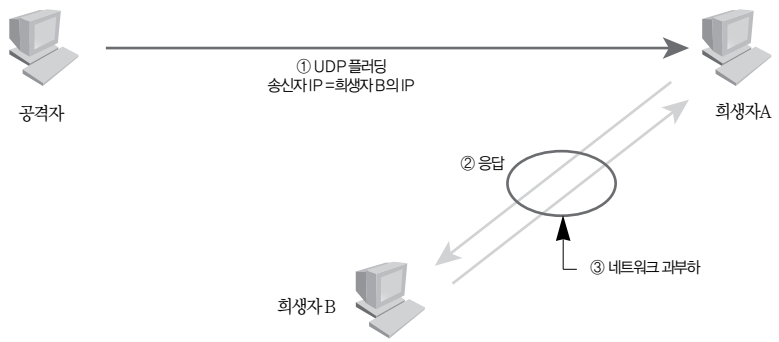
그림 4-3 SYN 플러딩에 의한 서비스거부공격



나. UDP 플러딩(UDP Flooding)

UDP 플러딩은 UDP의 비연결성 및 비신뢰성 때문에 공격이 용이한 방법이다. UDP는 소스 어드레스와 소스 포트를 spoofing하기 쉽다. 이러한 약점들을 이용해 (그림 4-4)와 같이 과다한 트래픽을 희생자(victim)에 전송함으로써 희생자간(희생자A, 희생자 B) 네트워크를 마비시킨다.

그림 4-4 UDP 플러딩에 의한 서비스거부공격



다. Smurf 공격(Smurf Attack)

Smurf 공격에서는 두 개의 희생자를 유발한다. (그림 4-5)와 같이 아무것도 모르고 공격하는 서브네트워크 A와 엄청나는 대량의 ICMP 패킷의 공격을 받는 희생자 B이다. A는 네트워크 다운이나 서비스 저하는 일어나지 않지만, 쓸모없는 서비스를 하게 된다. 또한 B는 네트워크가 다운된다. 공격자 C가 소스 주소를 B의 주소로 변조하여 A의 네트워크 전체로 ICMP 패킷을 보내면 A는 echo reply를 B로 보낸다. 이 때 A의 네트워크 범위에 따라서 B로 보내지는 echo reply 패킷의 양은 엄청난 양이 된다. Smurf 공격이라고 부르는 ICMP echo reply amplifier는 A 네트워크 주소를 목적지 주소로 갖는 echo 패킷 하나를 보냈는데 응답 패킷이 엄청난 양이 되어 B로 전송되므로 Amplifier 공격이라고도 한다.

그림 4-5 스머프(Smurf) 공격

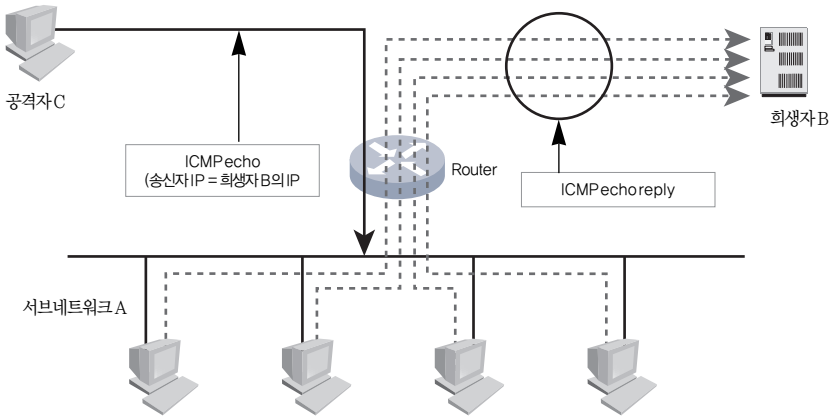
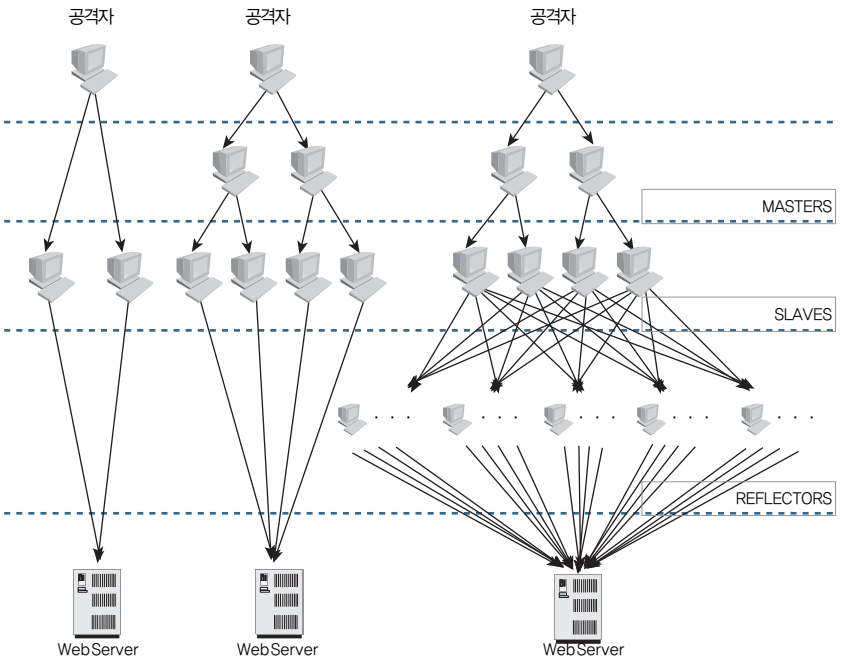


그림 4-6 분산 서비스 거부(DDoS) 공격



(A) Denial Service (DOS) 공격 **(B)** Distributed DOS (DDOS) 공격 **(C)** reflector를 이용한 DDOS 공격

라. 분산 서비스 거부 공격(DDoS)

분산 서비스 거부 공격은 일반적인 서비스 거부 공격을 보다 효과적이며 강력하게 공격하기 위한 방법으로 사용된다. 공격자의 추적이 일반적인 서비스 거부 공격보다 어려우며 더욱 강력한 공격을 할 수 있다. 먼저 공격자는 네트워크 상에서 보안이 허술한 시스템을 공격하여 관리자 권한을 획득하고 서비스 거부 공격을 위한 프로그램을 설치하는데 (그림 4-6)의 MASTERS와 SLAVES가 이러한 시스템에 해당하며, 이들도 분산 서비스 공격의 또 다른 희생자들이다.

또한 공격 유형을 감추고 추적이 어렵도록 공격 시 사용하게 될 명령들은 암호화하는 경우도 많다. 일반적인 침입탐지시스템이 암호화된 패킷을 점검하기 어렵다는 점을 악용하는 것이다.

1. IPSec을 이용한 대응방안

IPv6에서의 보안 기능은 IETF에서 개발된 IPSec에 의해 지원되며, IPv6 기반 IPSec이 제공할 수 있는 일련의 보안 서비스에는 접근제어, 무결성, 데이터 근원 인증, 재실행된 패킷 거부, 기밀성 등이 포함된다. 이 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 종단간의 안전한 통신을 지원하기 위해 IP 계층을 기반으로 하여 보안 프로토콜을 제공하는 개방 구조의 프레임워크로서 IP의 보안취약성을 보완하기 위한 보안 기능을 제공한다.

IPSec은 트래픽 보안을 위해 AH 및 ESP 프로토콜을 사용한다. AH 프로토콜은 무결성, 데이터 근원 인증 및 선택적 재실행 방지 서비스를 제공한다. ESP 프로토콜은 기밀성을 제공할 수 있다. 또한 무선접속의 무결성, 데이터 근원 인증 및 재실행 방지 서비스를 제공할 수 있다. IPSec으로 대응 가능한 공격은 [표 4-1]과 같다.

표 4-1 IPSec으로 대응 가능한 공격

공격유형 \ Protocols	AH	ESP
Replay	O SN	O SN
Packet 위,변조	O ICV	O ICV, Encryption
IP Spoofing	O ICV	O ICV
Packet sniffing	–	O Encryption
Session Hijacking	–	O ICV, Encryption
DoS	–	△ ICV, Encryption

※ SN : Sequence Number, ICV : Integrity Check Value

IPSec 표준은 안전한 IP VPN의 구축을 위한 핵심 요소 프로토콜 기술을 제공한다. 최근 들어, 재택근무나 출장지에서 본사 네트워크에 원격 접속 수요가 늘어남에 따라 VPN의 활용 범위가 넓어지고 있다. VPN의 구축 시 사용자 입장에서는 멀티 벤더 구축이 바람직하지만, 그동안 IKE 프로토콜의 상호 연동성 부족이 걸림돌이 되어 왔다. 그러나 IKEv2의 표준화로 상호 연동성이 제고되면, VPN의 구축 확산이 가속화될 것이다.

[표 4-2]는 IPSec 프로토콜의 특징을 정리한 것이다.

AH(Authentication Header)는 IP 데이터그램을 인증하기 위해 필요한 정보를 포함하는 방법으로 보안 효과, 특히 데이터의 인증과 무결성을 보장해 주는 메커니즘이다. AH는 다음의 보안 서비스를 제공 한다.

표 4-2 IPSec 프로토콜의 특징

구분	종류	설명
헤더	AH(Authentication Header)	– 비연결형 무결성/인증 서비스
	ESP(Encapsulating Security Payload)	– 비연결형 기밀성/무결성/인증 서비스
키 교환	IKE(ISAKMP/Oakley)	– 두 개체간의 인증 – 키 및 보안에 관련된 패러미터들을 협상 – 공유 비밀키(Pre-shared Secret) 또는 공인 인증서(Public Key Certificate) 기반
	Diffie-Hellman	– PFS(Perfect Forward Secrecy) 제공
모드	트랜스포트 모드	– 종단간 보안 서비스 – IP 헤더 제외한 부분에 대해서 보호 서비스 – 트래픽 분석에 취약할 수 있음 – 보안 외에 출발지와 도착지 주소를 기반으로 QoS(Quality of Service)를 제공할 수 있음
	터널 모드	– IP 헤더 포함한 전체에 대해서 보호 서비스 – 여러 호스트에 대해서 같은 터널을 쓸 수 있음 – 트래픽 분석에 대해서 보호 기능 – 비공인(사설) IP 주소를 사용할 수 있음
암호/인증 알고리즘	암호 알고리즘	DES, 3DES, RC5, IDEA, CAST, BLOWFISH, 3IDEA, RC4
	인증 알고리즘	MD5, SHA-1, DES

※ DES, SHA-1은 자체취약성으로 사용상 주의 필요

▶ **데이터의 무결성** : 메시지 인증을 담당하는 코드(Message Authentication Code)에 의해 계산된 각 필드의 합산 값을 수신자가 확인함으로써 보장된다.
▶ **데이터의 인증** : 인증 시 필요한 키와 인증 알고리즘을 SA와 연계하여 지정하고 지정된 알고리즘을 수행함으로써 보장된다.
▶ **재생공격 방지** : 인증 헤더에 있는 Sequence Number 필드의 값을 일련 번호화 함으로써 보장된다.

ESP(Encapsulating Security Payload)는 암호화 기법을 사용하여 데이터의 무결성, 리플레이 방지, 비밀성의 기능을 제공하는 프로토콜이다. 사용하는 암호알고리즘의 형태와 모드에 따라 인증 기능까지도 제공한다. 그러나 트래픽 분석을 통한 공격에 대한 보호와 부인 방지는 제공되지 않는다. 부인방지 등의 다양한 보안 서비스를 위해서 인증 헤더와 혼합해 사용되기도 한다.

IPSec 프로토콜에서 사용하는 모드에는 두 가지가 있는데 보호하는 데이터 영역에 따라 터널 모드와 트랜스포트 모드로 구분된다.

일반적으로 IPSec은 다음의 4가지 형태로 보안성을 제공해야 한다.

터널 모드는 일반적으로 패킷의 궁극적인 목적지와 보안 터널의 종단이 다를 때 사용한다. 따라서 터널의 종단이 보안 게이트웨이일 경우에는 항상 터널 모드를 사용해야 한다. 그러나 두 호스트 사이에서도 터널 모드 IPSec이 구성될 수 있다.

(그림 4-7)과 (그림 4-8)는 터널 모드에서의 패킷 구조 및 AH, ESP의 위치를 설명하고 있다.

트랜스포트 모드는 단대단 보안이 요구될 경우에 사용한다. 이 모드에서 AH와 ESP는 트랜스포트 계층에서 패킷의 변형을 통해서 트랜스포트 헤더 상위에 대한 보안성을 제공한다.

그림 4-7 터널 모드의 AH

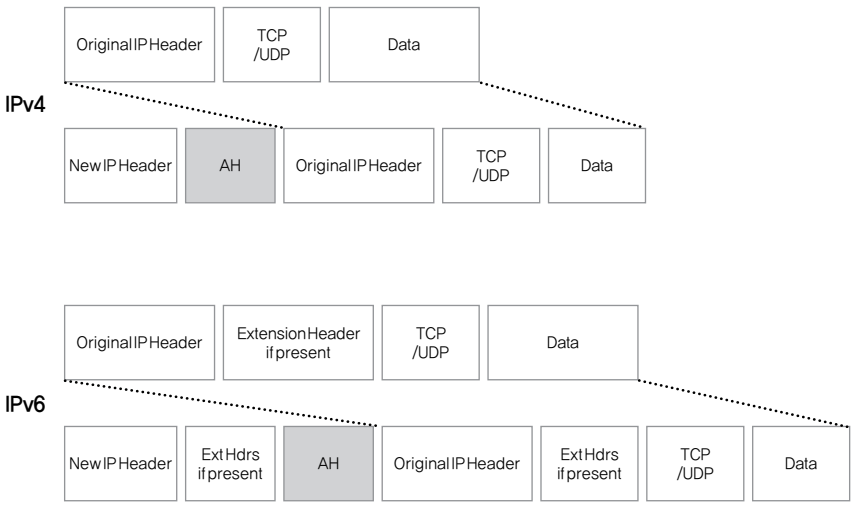
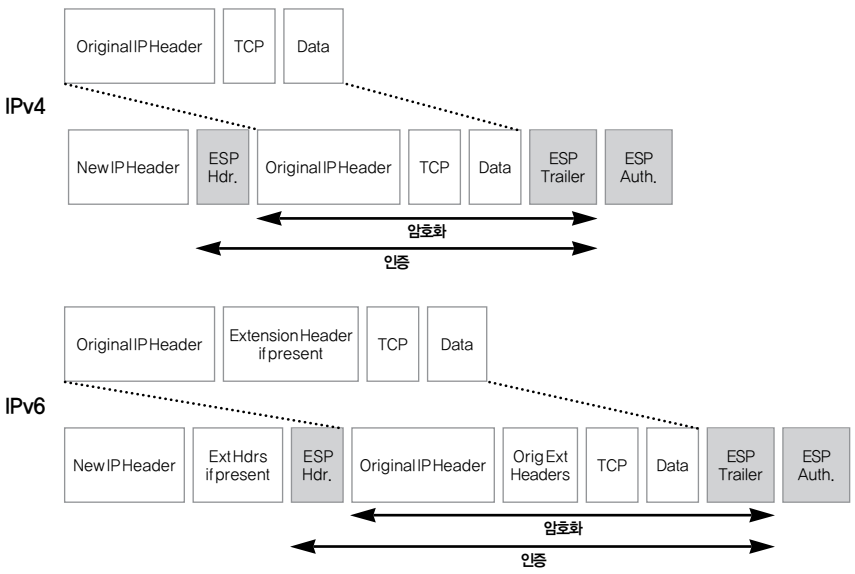


그림 4-8 터널 모드의 ESP



(그림 4-9)와 (그림 4-10)는 트랜스포트 모드에서의 패킷 구조 및 AH, ESP의 위치를 설명하고 있다.

그림 4-9 트랜스포트 모드의 AH

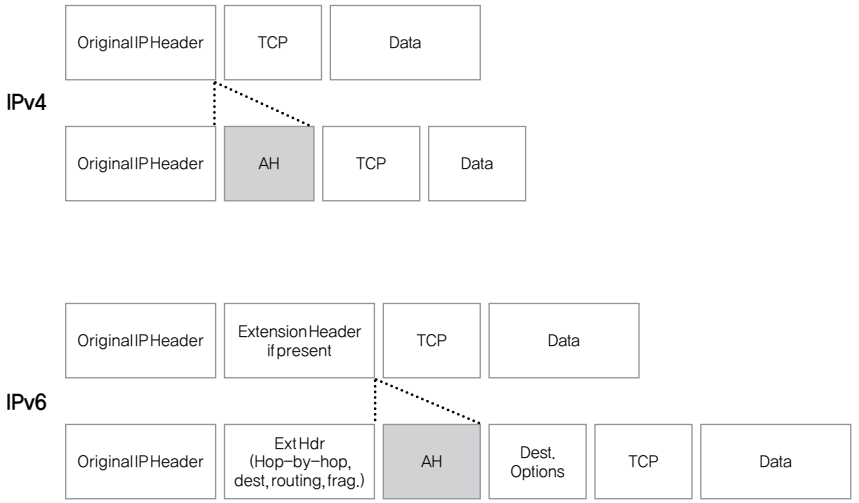
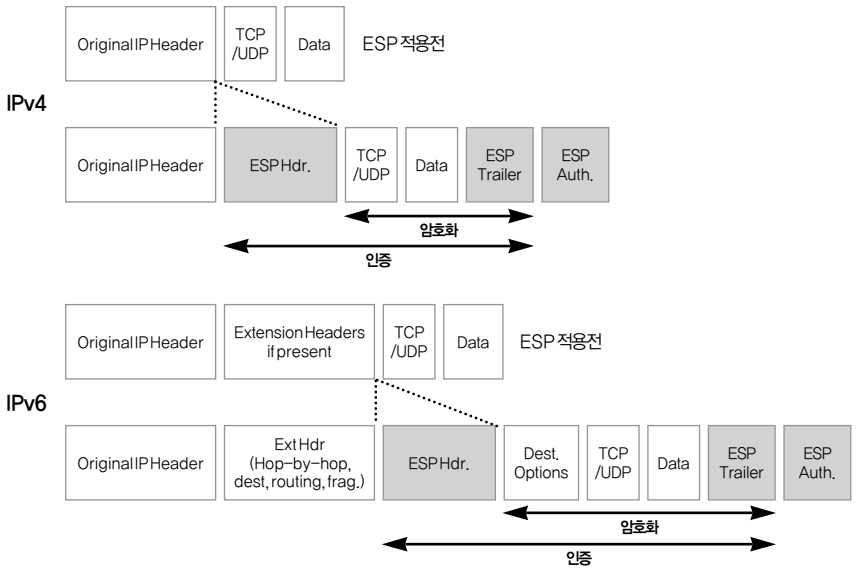


그림 4-10 트랜스포트 모드의 ESP



2. 침입차단시스템을 이용한 대응방안

가. 침입차단시스템의 구조

침입차단시스템은 보안정책을 적용하는 시스템으로 네트워크 경계에 위치하여 외부의 보안취약성들로부터 내부의 사설망을 보호한다. 또한 DMZ(DeMilitarised Zone)의 구성과 같은 특수한 목적을 위하여 사용될 수도 있다.

침입차단시스템은 [표 4-3]과 같이 네트워크의 계층을 비롯한 여러 계층에서 동작할 수 있으며, 서로 다른 계층에서 혼합하여 운용할 수 있다.

표 4-3 침입차단시스템의 동작 계층

계층	침입차단시스템 종류
네트워크 계층	패킷 필터링 침입차단시스템
전송 계층	서킷 지향적 침입차단시스템
어플리케이션 계층	어플리케이션 레벨 프록시

IPv6에서 사용하는 침입차단시스템이 IPv4와 기술적으로는 동일한 것이나 주소 표현 방식이 다르기 때문에 이와 관련된 수정 작업이 필요하고, 주소 자동 설정에 대한 대책 등 관리적인 이슈들이 적절히 반영되어야 한다.

나. 침입차단시스템의 위치

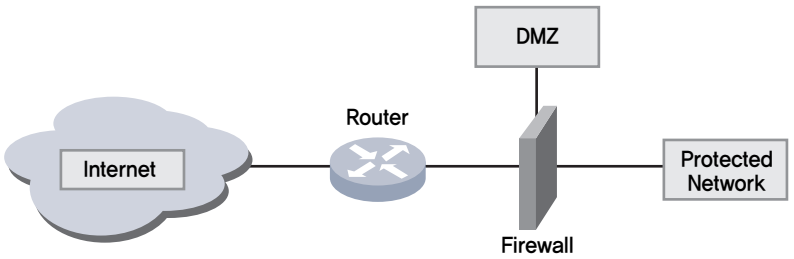
침입차단시스템은 각 네트워크에 한 개 이상이 설치되며 보호되어야 하는 네트워크나 장치 앞에 설치된다. IPv6상에 이러한 침입차단시스템이 운용될 수 있도록 하려면 다음과 같은 내용을 고려해야 한다.

▶ 침입차단시스템은 Neighbor Discovery 과 Neighbor Advertisement의 ICMPv6메시지를 처리할 수 있어야 한다. 또한, ARP 프로토콜의 확장인 NDP 필터링을 지원해야 한다.

▶ 관리자는 IPv6 침입차단시스템이 정상적인 'fragmentation' 헤더를 가진 외부 패킷을 필터링하지 않도록 주의하여 설정해야 한다. IPv4 침입차단시스템에서 단편화된 패킷에 tear-drop 공격 등을 보호하기 위해 IP패킷을 재조립하고 단말 시스템에게 완전한 정상적인 패킷을 전달한다. 그러나 IPv6에서는 패킷의 단편화 및 재조립이 단말 시스템에서만 가능하기 때문에 침입차단시스템에서의 필터링이 어렵다.

(그림 4-11)에서 (그림 4-13)은 침입차단시스템을 설치할 수 있는 위치를 보여주고 있으며, 이에 따른 고려사항들은 다음과 같다.

그림 4-11 라우터와 내부네트워크 사이에 위치

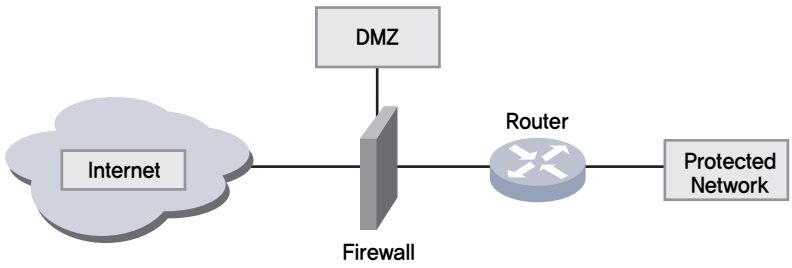


(그림 4-11)에서와 같이 구성된 경우, 주소자동설정이 사용된다면 침입차단시스템은 이를 지원해야 한다. 침입차단시스템이 네트워크 계층에 투명하게 운영된다면 호스트로부터의 'Router Solicitation' 메시지와 그에 대응하는 라우터로부터의 응답메시지를 차단해서는 안된다. 또한 라우터에서 내부 네트워크로 전송되는 주기적인 'Router Advertisement' 메시지를 허용해야 한다. 만약 침입차단시스템이 라우터와 내부 호스트간의 교환되는 메시지를 필터링한다면, 침입차단시스템 자신이 'Router Solicitation' 메시지들에 응답할 수 있어야 하고 주기적으로 'Router Advertisement' 메시지를 내부 호스트들에게 전송해야 한다. 내부 네트워크가 DHCPv6를

운영하고 있다면 이러한 설정은 매우 중요하다.

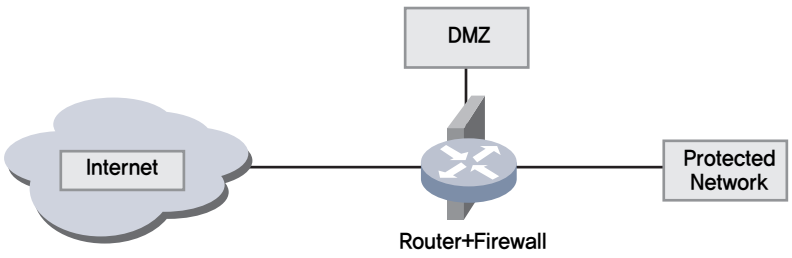
내부 네트워크 내의 IPv6 멀티캐스트 그룹에 참가하고 있는 멤버가 존재한다면 침입차단시스템은 MLD(Multicast Listener Discovery)프로토콜을 지원해야 한다.

그림 4-12 인터넷과 내부네트워크의 라우터 사이에 위치



(그림 4-12)에서의 침입차단시스템은 라우터에서 사용되는 동적 라우팅 프로토콜에 대한 필터링 기능을 지원해야 한다. 그러나 IPSec이 사용될 때에는 BGP가 보안 라우팅 업데이트를 위해 MD5 해시를 사용하기 때문에 정적인 라우팅 기법을 사용하도록 하고있다.

그림 4-13 라우터와 침입차단시스템이 통합된 경우



(그림 4-13)의 구조는 한 장치에 두 기능을 통합하기 때문에 좀 더 복잡하고 더 많은 보안문제에 직면할 수 있다. 이러한 설정은 작은 사무실의 환경에서 사용되는 구조이다. 이에 따라 (그림 4-11)과 (그림 4-12)에서의 고려사항을 모두 만족해야 한다.

다. 침입차단시스템이 설치된 IPv6환경에서 주소 사용 및 할당

침입차단시스템이 설치된 IPv6 환경에서 주소를 할당하는 방법들은 아래와 같다.

▶ **비상태형 주소자동설정**(stateless address auto-configuration) : 글로벌 유니캐스트 주소는 라우터가 광고한 프리픽스정보와 IEEE EUI-64형식의 식별자를 이용하여 설정된다. EUI-64 식별자는 MAC주소로부터 유도될 수 있기 때문에 IP주소와 MAC주소의 맵핑이 용이하다. 이 때, 침입차단시스템은 MAC 주소와 L2포트간의 매핑을지원할 수 있어야 한다. 침입차단시스템에서는 이미 외부네트워크으로 전송되는 패킷들의 MAC 주소와 EUI주소의 지속성을 체크할 수 있으나 정적으로 할당되는 주소들을 사용하는 경우에는 주소정보가 수동적으로 설정되어 있어야 한다.

▶ **DHCPv6** : DHCPv6(Dynamic Host Configuration Protocol version 6)는 상태정보를 유지하는 주소자동설정 프로토콜이다. DHCPv6 서버들은 설정 파라미터들에 대한 클라이언트들과 IA(Identity association) 클라이언트들과 관련된 클라이언트를 식별하기 위해 DUID(Dhcp Unique IDentifier)를 사용한다. DHCP 클라이언트는 서버를 식별할 필요가 있는 메시지에서의 서버를 식별하기 위해 DUID를 사용한다. 침입차단시스템은 DHCPv6를 사용하여 DUID를 설정한 내부 호스트만이 외부 네트워크의 호스트와 연결이 가능하도록 해야 한다.

▶ **정적 주소 할당** : 정적 주소 할당은 IPv4의 정적 주소할당기법과 매우 유사하므로 사용할 경우 IPv4에서의 보안취약성과 유사하다.

DHCPv6를 사용하여 주소를 할당하는 경우, 침입차단시스템은 DHCPv6를 모니터링하여 주소의 오남용을 방지할 수 있다. 또한 비상태 주소자동설정의 경우, 주소 및 포트의 오남용을 방지하기 위해 'Neighbor Solicitation' 메시지와 'Neighbor Advertisement' 메시지의 모니터링을 이용할 수 있다. 'Neighbor Solicitation' 메시지들은 [소스 IPv6 주소, 소스 MAC 주소]를 가지고 있는 반면, 'Neighbor Advertisement' 메시지는 [소스 IPv6, 소스 MAC 주소]와 [목적지 IPv6, 목적지 MAC 주소] 정보를 가지고 있다. 두 메시지가 가진 주소 정보가 일치되지 않은 경우에는 이전의 저장된 ND 엔트리로부터 분석하여 스위치의 포트 남용을 방지할 수 있다. 따라서 침입차단시스템은 같은 MAC주소를 가진 다른 IP주소의 ND엔트리의 변화를 감지할 수 있어야 한다.

제 5 장 결론

기존 IPv4 프로토콜은 보안을 고려하여 설계하지 않았기 때문에, 다양한 보안공격에 노출되어 있는 반면에 IPv6에서는 IPSec을 기본으로 제공하고 있기 때문에 다양한 공격을 상당부분 해결할 수 있다.

그러나, IPv6에서 제공하는 자동설정, 확장헤더 등 새로운 기능들은 공격자에 의해 악용될 수 있는 보안취약성을 갖고 있다. 대부분의 사람들이 IPv6의 보안을 위한 기술로 IPsec만을 언급하고 있지만, 아직까지 복잡한 설정 및 키 관리 문제를 완전히 해결하지 못하고 있기 때문에 모든 새로운 IPv6 보안공격에 대한 대응방안으로 사용하기에는 부족하다.

본 안내서는 IPv6가 가지고 있는 새로운 기술과 그 기술의 보안취약성을 분석하고 대응방안을 설명하였다. 또한 전국적인 규모의 IPv6 네트워크 구축이 완료되기까지 IPv4와 IPv6가 혼재되어 공존할 것으로 예상됨에 따라, IPv4/IPv6 전환기술에 대한 보안취약성 분석 및 대응방안을 설명하였고, 마지막으로 IPv4와 IPv6에 공통적으로 발생할 수 있는 보안공격에 대한 대응방안을 설명하였다.

또한 이동환경에서의 보안취약성 분석 및 대응방안 설명을 통하여 향후, Mobile-IPv6 환경에서의 활용성을 고려하였다.

네트워크 관리자는 본 기술안내서를 활용하여 안전한 IPv6 네트워크 구축 및 운영에 대한 정보를 습득함과 함께 IPv6 보안취약성에 대해 효과적인 대응방안을 수립할 수 있을 것이다.

부 록

A. IPv6 주소 검증을 위한 CGA기법

CGA 기법은 IPv6 주소의 일부정보가 노드의 공개키로 유도될 수 있다는 것에 기반하고, 장점은 인증서가 필요 없다는 것이다. 이는 공개키 기반 구조가 요구되지 않고 키소유자가 필요시 공개키를 생성한다.

IPv6 주소의 길이는 128비트이며 64비트의 네트워크 프리픽스 정보와 64비트의 인터페이스 식별자로 구성된다. 네트워크 프리픽스는 네트워크에서 라우팅시 사용되며 링크상에 특정노드는 링크상에 유일한 인터페이스 식별자에 의해 찾을 수 있다.

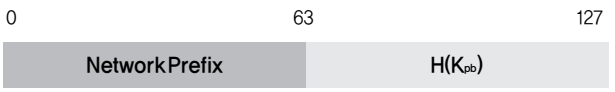
인터페이스 식별자는 기본적으로 MAC주소를 이용하여 생성된다. 하지만 대부분의 모든 값들이 사용될 수 있으며 오직 2비트만이 특별한 의미를 갖는다. 다시 말해서 62비트의 인터페이스 식별자는 링크상에 유일한 값이 있는 경우 그 값을 이용하여 어떤 기법에 의해서도 생성될 수 있다. 이러한 유일성은 IPv6의 DAD(Duplicate Address Detection) 알고리즘에 의해 보장된다.

표 A-1 CGA 인증에 사용되는 변수정의

기호	정의	기호	정의
K_{pb}	MN의 공개키	K_{pr}	MN의 개인키

CGA기법은 [표 A-1]에서의 노드의 공개키 K_{pb}으로부터 IPv6 주소의 인터페이스 식별자를 유도한다. 이는 (그림 A-1)과 같은 64비트값을 반환하는 해시함수에 의해 생성될 수 있다.

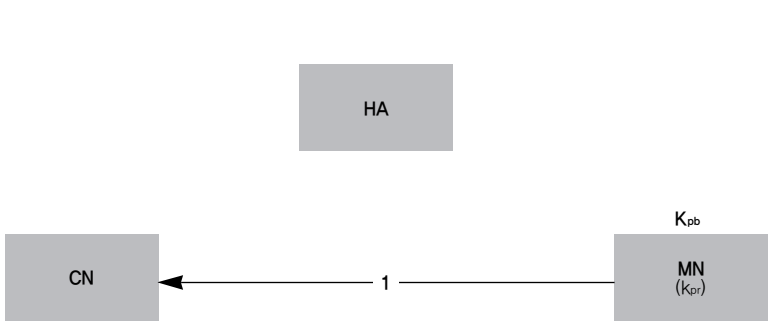
그림 A-1 CGA를 이용한 IPv6 주소



이제 바인딩 업데이트 메시지는 (그림 A-2)와 같이 생성될 수 있다. 바인딩 업데이트 메시지를 수신한 후, CN은 공개키 K_{pb}을 가진 노드로부터 온 것인지를 확인하는 것은 HoA가 K_{pb}으로부터 유도되었음을 검증하여 알 수 있다. K_{pb}의 유효성은 공개키로부터 유도된 CGA주소로 생성한 주소와 수신한 메시지의 HoA와 비교하여 확인할 수 있다. 이후 CN은 서명을 검증하여 실제 MN으로부터 온 메시지인지를 확인할 수 있다. 서명은 해시된 값을 계산하여 수신된 메시지에서 공개키 K_{pb}을 이용하여 복호화한 값과 동일한지를 검증할 수 있다.

바인딩 확인과 바인딩 요구 메시지 또한 CGA기법을 통하여 인증할 수 있으나, CN은 반드시 CGA를 사용하고 있어야 한다.

그림 A-2 CGA를 이용한 바인딩 업데이트 인증



약 어

AH	Authentication Header
ALG	Application Layer Gateway
AR	Authentication Request
BA	Binding Acknowledgement
BFD	Bidirection Forwarding Detection
BGP	Border Gateway Protocol
BR	Binding Request
BU	Binding Update
CGA	Cryptographically Generated Address
CN	Correspondent Node
CoA	Care of Address
DHCP	Dynamic Host Configuration Protocol
DSTM	Dual Stack Transition Mechanism
DTI	Dynamic Tunnel Interfaces
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GCKS	Group Controller/Key Server
GDOI	Group Domain of Interpretation
GPL	GNU General Public License
GRE	Generic Route Encapsulation
HA	Home Agent
HAO	Home Address Option
HN	Home Network
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6

IKE	Internet Key Exchange Protocol
IPSec	Internet Protocol Security
ISATAP	Intra Site Automatic Tunnel Address Protocol
IS-IS	Intermediate System-to-Intermediate System
ISP	Internet Service Provider
KDC	Key Distribution Center
MIB	Management Information Base
MIPv6	Mobile IPv6
MN	Mobile Node
MTU	Maximum Transmission Unit
NAPT-PT	Network Address Port Translation- Protocol Translation
NAT	Network Address Translation
NAT-PT	Network Address Translation-Protocol Translation
NDP	Neighbor Discovery Protocol
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
QoS	Quality of Service
RA	Router Advertisement
RDoS	Reflection of Denial-of-Service
RIPng	Routing Information Protocol next generation
RPF	Reverse Path Forward
RR	Return Routability
RS	Router Solicitation
RTT	Round Trip Time
SA	Security Association

SAD	Security Association Database
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
TLS	Transport Layer Security
TSP	Tunnel Setup Protocol

참고문헌

[1] "A Discussion on IPv6 Transition Mechanisms", IPv6style in Japan, 2003

[2] "Anycast security requirements", Secure Multicast Group

[3] "Changing the Default for Directed Broadcasts in Routers", RFC 2644, 1999

[4] "Characteristics of Fragmented IP Traffic on Internet Links", 2001

[5] "Child-proof Authentication for MIPv6 (CAM)", Microsoft Research Ltd

[6] "Cisco IOS Configuration Guide, Release 12.4T", http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a00801d65f4.html

[7] "Dual Stack Transition Mechanism (DSTM)", draft-ietf-ngtrans-dstm-08.txt

[8] "Firewalling Considerations for IPv6", draft-savola-v6ops-firewalling-01.txt

[9] "Identifiers and Addresses", draft-montenegro-sucv-02.txt

[10] "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, 1998

[11] "Inside the Slammer Worm", http://www.caida.org/outreach/papers2003/sapphire2/

[12] "IPv4/IPv6 Coexistence with Application Perspective", Global IPv6 Summit

[13] "IPv6 Distributed Security Requirements", draft-palet-v6ops-ipv6security-02.txt

[14] IPv6 Security Links, http://www.seanconvery.com/ipv6.html

[15] "IPv6 Transition mechanisms", ngnet.it

[16] "IPv6 Transition/Co-existence Security Considerations",

[17] "IPv6 IPSec 기술 및 동향", Future System, 2005

[18] "IPv6 동향 2004", 한국전산원, 2005

[19] "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-16.txt

[20] "Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, 2000

[21] "Privacy Extensions for Stateless Address auto-configuration in IPv6", RFC 3041, 2001

[22] "Protecting Against Bidding Down Attacks", draft-montenegro-mipv6sec-bit-method-00.txt

[23] "Review of IPv6 Transition Scenarios for European Academic Networks", IPv6 Conference, 2002

[24] "Security and IPv6", http://www.ipv6.bt.com/tutorials/security.html

[25] "Security Architecture for the Internet Protocol", RFC 2401, 1998

[26] "Security Considerations for 6to4", draft-ietf-v6ops-6to4-security-00.txt, draft-savola-v6ops-security-overview-03.txt

[27] "Security Implications of IPv6", Internet Security Systems

[28] "Security of IPv6 Routing Header and Home Address Options", draft-savola-ipv6-rh-ha-security-03.txt, 2002

[29] "Unmanaged Networks IPv6 Transition Scenarios", RFC 3750

[30] 6NET, http://www.6net.org

[31] DSTM(Dual Stack Transition Mechanism) http://www.dstm.info/

본 안내서의 작성을 위하여 다음과 같은 분들께서 수고 하셨습니다.

2010년 2월

총괄 책임자	**한국인터넷진흥원 인 터 넷 융 합 단**	**단 장**	**이 재 일**
	인 터 넷 정 책 단	**단 장**	**원 유 재**
	융합보호R&D팀	책임연구원	윤 미 연
	기업보안관리팀	선임연구원	오 규 철
	융합보호R&D팀	책임연구원	지 승 구

안내서를 검토하여 주신 한선영(건국대), 강현국(고려대), 김형식(충남대), 정영조(퓨쳐시스템), 김유정(한국정보화진흥원), 나재훈(ETRI), 김형준(ETRI), 박용범(TTA) 님께 감사드립니다.

《 한국인터넷진흥원(KISA)『안내서·해설서』시리즈 》

분류	안내서·해설서	해당팀명	발간년월	대상	수준
인터넷 진흥	DNS 설정 안내서	시스템관리팀	'09년	IT시스템관리자	중급
	인터넷주소분쟁해결 안내서	도메인팀	매년발간 offline	일반	초급
	모바일 RFID코드 및 OID기반 RFID코드 적용 안내서	무선인터넷팀	'09.8	IT기업개발자	중급
	13.56MHz대역의 OID적용을 위한 미들웨어 개발 안내서	무선인터넷팀	'09.12	IT기업개발자	중급
	공공기관 IPv6 적용 안내서	IP팀	'08.12	IT시스템관리자	중급
인터넷 이용 활성화	본인확인제 안내서	인터넷윤리팀	'09.2	일반 · 업무관계자	중급
	본인확인제 만화 안내서	인터넷윤리팀	'09.	일반	초급
정보보호 시스템 관리	BcN 정보보호 안내서	인터넷서비스 보호팀	'07./ '10.1	IT시스템관리자	중급
	침해사고 분석절차 안내서	해킹대응팀	'10.1	IT시스템관리자	고급
	웹서버구축 보안점검 안내서 웹어플리케이션 보안 안내서 홈페이지 개발보안 안내서	웹보안지원팀	'10.1	IT시스템관리자	고급
	무선랜 보안 안내서	해킹대응팀	'08.10/ '10.1	일반	중급
	침해사고대응팀(CERT) 구축/운영 안내서	상황관제팀	'07.9	업무관계자	중급
	WebKnight를활용한 IIS 웹서버 보안 강화 안내서 WebKnight 로그 분석 안내서 ModSecurity를 활용한 아파치 웹서버 보안 강화 안내서	웹보안지원팀	'09.6	IT시스템관리자	중급
	보안서버구축 안내서	개인정보보호팀	'08.7	IT시스템관리자	중급
정보보호 인증	IT보안성 평가 · 인증 안내서	공공서비스보호팀	'09.12	일반 · 업무관계자	초급
기업 정보보호	정보보호 안전진단 해설서	기업보안관리팀	'08.4/ '10.1	업무관계자	초급
	정보보호 안전진단 업무 안내서	기업보안관리팀	'10.1	업무관계자	초급
	정보보호관리체계 안내서	기업보안관리팀	'09.12	일반	초급
신규 서비스 정보보호	패스워드 선택 및 이용 안내서	융합보호R&D팀	'10.1	일반	초급
	암호이용 안내서	융합보호R&D팀	'07.12/ '10.1	일반	중급
	IPv6운영보안 안내서	융합보호R&D팀	'06.12	IT시스템관리자	중급
	IPv6보안기술 안내서	융합보호R&D팀	'05.	일반	초급
	와이브로 보안기술 안내서	융합보호R&D팀	'06.8	IT시스템관리자	중급
	암호 알고리즘 및 키 길이 이용 안내서	융합보호R&D팀	'07	IT시스템관리자	중급
	(기업 및 기관의 IT 정보자산 보호를 위한) 암호정책 수립 기준 안내서	융합보호R&D팀	'07	IT기업개발자	중급
	(정보의 안전한 저장과 관리를 위한) 보조기억매체 이용 안내서	융합보호R&D팀	'09	일반	초급
	웹사이트 회원탈퇴 기능 구현 안내서	융합보호R&D팀	'06	IT시스템관리자	중급
개인정보	개인정보의 기술적 · 관리적 보호조치 기준 해설서	개인정보보호 기획팀	'09.9	업무관계자	중급
	위치정보의 보호 및 이용 등에 관한 법률 해설서	개인정보보호 기획팀	'08.12	업무관계자	중급
	위치정보보호를 위한 관리적·기술적 보호조치 권고 해설서	개인정보보호 기획팀	'08.11/ '10.1	업무관계자	중급
	웹사이트 개발 · 운영을 위한 개인정보 안내서	개인정보보호 기술팀	'09.11	IT기업 개발자 · 관리자	중급
	I-PIN 2.0 도입 안내서	개인정보보호 기술팀	'09.7	업무관계자	중급
	김대리, 개인정보보호 달인되기	이용자권익보호팀	'09.8	업무관계자	중급
	기업의 개인정보영향평가 수행을 위한 안내서	이용자권익보호팀	'09.1	업무관계자	중급
스팸	사업자를 위한 불법스팸 방지 안내서	스팸대응팀	'08.9	일반 · 업무관계자	초급
인력 양성	지식정보보안 신규일자리 창출사업 세부시행 안내서	KISA아카데미팀	'09.	업무관계자	초급
	총40종				

IPv6 보안 기술 안내서

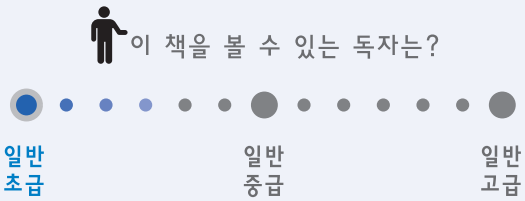
2010년 2월 인쇄
2010년 2월 발행

발행처: **한국인터넷진흥원**

서울특별시 송파구 가락동 79-3번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-4118

인쇄처: 한올
Tel: (02) 2279-8494

<비매품>



한국인터넷진흥원

138-950 서울시 송파구 가락동 79-3번지 대동빌딩
Tel. 405-4118 Fax. 405-5119
www.kisa.or.kr