주 제

IPv4/IPv6 변환기 보안 위협

숭실대학교 김미영, 문영성

차 례

요 약

인터넷의 급속한 보급으로 다양한 영역(휴대용 랩톱, PDA등의 이동 단말, 센서 네트워크, 3G/3GPP와 같은 이동 통신망 등)에서 IP 기반 통신환경이 요구되고 있으며, 이를 충족시키기 위한 다양한 연구가 진행되고 있다. IPv6 프로토콜의 주요 특징으로는 '풍부한 주소 공간', '헤더 처리의 효율성', '보안성 제공', '이동성 제공' 및 '주소 관리의 효율성 제공' 등이 있지만, 아직까지 킬러 어플리케이션의 부재, 통신 사업자와의 이해관계 및 투자 보존 등과 같은 이유로 기존의 IPv4 인프라를 모두 대체하는 데 한계가 있다. 따라서 상당기간 IPv4 네트워크와 IPv6 네트워크가 공존하는 상태에서 IPv6 네트워크로 진화할 것으로 예상하고 있다. 본 연구에서는 IPv4/IPv6 공존 망에서 서비스 사용에 대한 보안 문제점을 분석하였다.

I. 연구 배경

현재 사용하고 있는 IPv4 프로토콜의 주소체계는 32비트 주소체계이므로 이론적으로 232개(약 43억개)의 주소를 만들 수 있다.[1] 그러나 A 클래스는 전체 128개의 네트워크만을 구성할 수 있으므로 미국을 중심으로 대부분 할당되어 고갈된 상태이고, E 클래스는 연구용으로만 사용된다. C 클래스는 구성할 수 있는 네트워크의 수는 많지만 하나의 C 클래스 네트워크에 연결 가능한 호스트의 개수가 매우 적으므로 소규모의 빌딩이나 기업체 등에 사용된다. 따라서 설정 가능한 네트워크와 호스트의 수가 동일한 B 클래스의 IP주소를 선호함에 따라 급속히 고갈되어 가고 있다. 이는 초기 IP 주소 설계 시 수요를 충분히 예측하지 못한 이유에서 비롯되었는데, IP 주소는 초기의 비효율적인 주소 할당과 인터넷의 급격한 발달 및 첨단 인프라에 따른 고도의 디지털 서비스 지원을

위한 주소 수요의 급증으로 한계점에 근접하고 있다. 전문가들에 의하면 IPv4 주소는 2022년이면 완전히 고갈될 것으로 예측되고 있다.

이러한 주소부족 문제를 해결하기 위한 임시적인 해결책으로는 주소 공간을 효율적으로 재구성하는 CIDR(Classless Inter-Domain Routing), NAT(Network Address Translation), DHCP (Dynamic Host Configuration Protocol) 등을 이용한 방식이 있다. 그러나 NAT사용 시 네트워크의 보안성을 향상시키는 반면, 인터넷 종단 노드간의 직접적인 통신을 방해한다. DHCP를 사용한 주소 할당 방법의 장점은 주소를 할당하고 사용이 종료되면 다른 노드에 할당함으로써 주소 사용의 효율성을 높일 수 있지만, 고정적인 IP 사용을 원하는 노드의 경우 DHCP를 사용할 수 없고, 망 내부에 두 가지 방법이 혼재하는 경우 관리의 혼선을 가져올 수 있다. 궁극적으로 주소 고갈을 막는 해결책이 되지 않으므로 인터넷 주소 제공 및 관리를 위한 장기적으로 근본적인 해결을 위해 IPv6 프로토콜로의 전환이 시급하다.[2]

향후 무선 인터넷 통신망 및 인터넷 정보가전의 도입에 따라서 IP 주소의 수요가 폭발적으로 증가 할 것으로 추정된다. 따라서 IPv4 주소로는 급증하는 주소 자원의 수요를 충족시킬 수 없기 때문에 IPv6 주소체계로의 전환이 절실히 요구된다. 인터넷은 데이터서비스 뿐만 아니라 전화, 방송 등 기존의 정보통신서비스를 전송할 수 있는 기술적 기반을 이미 확보하고 있다. 이동통신망이 유선 ISP(Internet Service Provider)망과 연동이 되도록 IPv6 네트워크로 점차 전환되면서 2010년 이후에는 All-IPv6 망으로 발전할 전망이다. 이에 따라 대부분의 네트워크가 IP 프로토콜을 수용하면서 인터넷은 모든 정보통신 서비스를 전송하는 종합 전달 망으로 발전할 전망이다. All-IP 시대를 준비하기 위해서는 현재의 IPv4 프로토콜로는 서비스 수용에 한계가 예상되므로 IPv6 프로토콜로의 전환이 필수적이다. 또한 가정 내 PC 주변장치의 다수 보유, 정보가전의 등장 및 가입자망의 전송 속도 향상에 따라 홈네트워킹 구축의 필요성이 증대되고 있다. LAN, PLC, RF 등을 활용한 홈 네트워크에 PC, 냉장고, TV 등의 장비를 연결하여 다양한 응용서비스를 제공할 수 있다. 향후 홈 네트워크가 활성화될 경우 사용자가 인터넷을 통하여 정보가전 기기들에 접속하고 통제하기 위해 IP 주소의 필요성은 급격히 증가함에 따라 IPv6 프로토콜은 선택이 아닌 필수 요건으로 인식되고 있다.

IPv6 프로토콜의 주요 특징으로는 '풍부한 주소 공간', '헤더 처리의 효율성', '보안성 제공', '이동성 제공' 및 '주소 관리의 효율성 제공' 등이 있지만[1] 아직까지 킬러 어플리케이션의 부재, 통신 사업자와의 이해관계 및 투자 보존 등과 같은 이유로 기존의 IPv4 인프라를 모두 대체하는 데 한계가 있다. 따라서 상당기간 IPv4 네트워크와 IPv6 네트워크가 공존하는 상태에서 IPv6 네트워크로 진화할 것으로 예상하고 있다. 이러한 과도기는 서비스의 자연스런 이전을 위해 필수 불가결한 단계로 해석할 수 있으며, 완전한 IPv6 네트워크에서 서비스 제공에 대한 사전 시험 및 평가 기간으로 활용될 수 있다.

본 연구에서는 IPv4/IPv6 변환 기술을 적용한 서비스 운용 시 발생할 수 있는 보안 문제점을 분석하였는데 주로 터널링 기술에 관한 보안 위협 및 공격 방법에 대해 기술하였다.

II. IPv4/IPv6 변환기술 동향

모든 IPv4 네트워크가 IPv6 네트워크로 전환되기 전까지 IPv4/IPv6 전환기술이 전 세계적으로 사용될 것으로 예상되며, 이러한 네트워크 환경에 적용할 수 있는 다양한 네트워크 기술에 대한 연구가 요구된

다. 지금까지 학계와 산업계에서 연구된 IPv4/IPv6 전환기술로는 Dual Stack, 6개의 Tunneling 기술(6in4, 6to4, ISATAP, DSTM, Teredo, Tunnel Broker), 그리고 6개의 Translation 기술(SIIT, NAT-PT, TRT, SOCKs gateway, BIS, BIA)이 있다. 이러한 기술들은 다양한 사용자의 컴퓨팅 환경과 요구사항을 충족시키기 위하여 제안 및 개발되었으며, 대부분의 기술이 IETF에서 RFC 문서로 표준화가 완료되었다.

〈표 1〉 Dual Stack, Tunneling 기술, 그리고 Translation 기술의 RFC 현황

구 분		RFC 현황
Dual Stack		RFC4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
Tunneling	6in4	RFC4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
	6to4	RFC3056: Connection of IPv6 Domains via IPv4 clouds
	ISATAP	RFC4214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
	DSTM	Internet-Draft: Dual Stack IPv6 Dominant Transition Mechanism
	Teredo	RFC4380: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
	Tunnel Broker	RFC3053: IPv6 Tunnel Broker
Translation	SIIT	RFC2765: Stateless IP/ICMP Translation Algorithm (SIIT)
	NAT-PT	RFC2766: Network Address Translation - Protocol Translation (NAT-PT)
	TRT	RFC3142: An IPv6-to-IPv4 Transport Relay Translator
	SOCKs gateway	RFC3089: A SOCKS-based IPv6/IPv4 Gateway Mechanism
	BIS	RFC2765: Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)
	BIA	RFC3338: Dual Stack Hosts Using "Bump-in-the-API" (BIA)

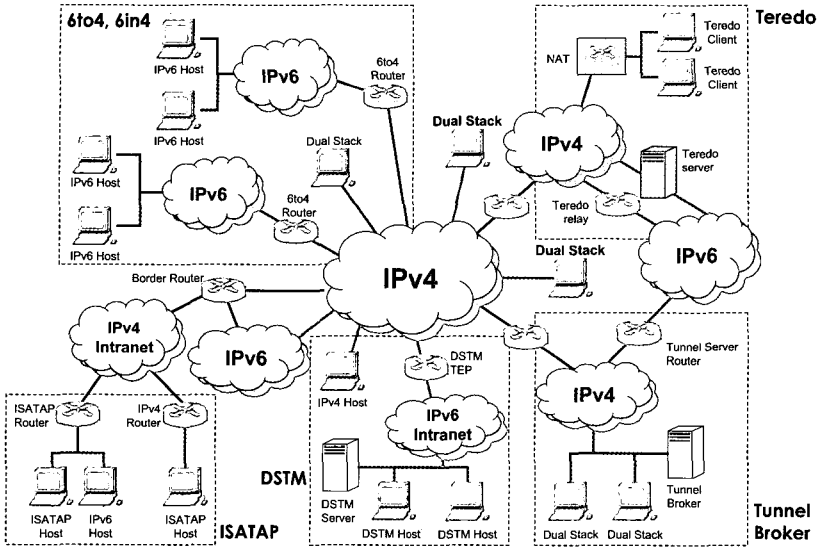
<표 1>에서 보이는 IPv4/IPv6 전환기술 중에서, 네트워크 간 연계 측면에서 가장 많이 사용될 것으로 예상되는 기술은 Dual Stack과 Tunnel 기술이다.[3] [4] <표 2>는 듀얼 스택과 터널링 기반의 전환 기술에 관한 기본 개념과 유용성에 관해 정리한 것으로서 현재 대부분의 운영체제에서 제공되는 기술들이다.

〈표 2〉 Dual Stack과 Tunneling 기술의 기본 개념과 유용성

구 분		기본 개념	유용성
Dual Stack		하나의 시스템에서 IPv4와 IPv6 프로토콜과 통신을 동시 처리할 수 있는 호환성 필요	하나의 시스템에서 IPv4와 IPv6 프로토콜과 통신을 동시 처리할 수 있는 호환성 필요
Tunneling	6in4	수동 터널링 방식으로 IPv4 망을 통하여 IPv6 패킷 통신	필요관리자 설정에 의해 정적 터널 유지 및 라우터 사이의 터널 연결에 유용
	6to4	동적 터널링 방식으로 IPv4 망을 통하여 IPv6 패킷 통신 필요	필요 시 자동 터널 생성 및 호스트 간 터널 연결에 유용
	ISATAP	IPv4 인트라넷에 있는 Dual Stack 호스트가 IPv4 인프라를 통해 IPv6 메시지 자동 터널링	IPv4 기반의 인트라넷에서 IPv6 호스트 설치 가능
	DSTM	IPv6 호스트가 IPv4 호스트 및 어플리케이션 이용 필요	IPv4 전용 어플리케이션의 수정 불필요
	Teredo	IPv4 NAT 내부에서 사설 IP를 이용하는 호스트가 IPv6 호스트와 통신 필요[5]	인터넷 공유기를 사용하는 가정이나 소규모 기업에서도 IPv6 통신 가능
	Tunnel Broker	Tunnel Broker라는 전용 서버를 구축하여 사용자의 터널 요청을 자동으로 관리	관리자에 의한 설정 터널링을 자동으로 관리함으로 관리 오버헤드 감소

또한 이러한 운영체제 이용하여 IPv4/IPv6 전환기술이 적용된 네트워크를 구성하였을 경우, 전체적인 네트워크 구성 도는 (그림 1)과 같다.

이와 같은 IPv4/IPv6 전환기술은 모든 IPv4 네트워크가 IPv6 네트워크로 전환되기 전까지 과도기적인 기술에 해당하지만, IPv6 네트워크가 활성화되기 전까지 IPv4 네트워크와 IPv6 네트워크가 공존하는데 있어서 상당히 많은 영역에서 필요한 기술이다.



(그림 1) IPv4/IPv6 전환기술이 적용된 네트워크 구성도

III. 터널링 기술 개요

3.1 6in4

'6in4'는 Pv4 네트워크에서 IPv6 네트워크로의 전환 과정에서 IPv6 프로토콜을 지원하지 않는 IPv4 네트워크 내에서 고립된 IPv6 네트워크나 IPv6 호스트들이 IPv4 네트워크를 이용하여 서로 통신할 필요성을 해결하기 위한 기술로서 표준문서 "RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers와 Internet-Draft 6in4 versus 6over4 terminology" 에서 IPv6 전환기술 중 하나로써 정의되어 있는 6in4는 IPv4 라우팅 인프라를 통해 전송되도록 IPv6 패킷을 IPv4 헤더 내에 캡슐화 함으로써 이루어지는 터널을 이용하는 방식이다. 이 기술은 IPv4 주소를 통해 수동으로 정적 터널을 설정한다.[6] [7]

3.2 6to4

'6to4'는 IPv4 네트워크에서 IPv6 네트워크로의 전환 과정에서 IPv6 프로토콜을 지원하지 않는 IPv4 네트워크 내에서 고립된 IPv6 네트워크나 IPv6 호스트들이 IPv4 네트워크를 이용하여 서로 통신할 필요성을 해결하기 위하여 제시된 기술로서 표준문서 "RFC3056: Connection of IPv6 Domains via IPv4 Clouds에 IPv6" 전환기술 중 하나로써 정의되어 있는 6to4 기술은 '2002::/16'의 고유한 라우팅 프리픽스로 시작하는 6to4 주소에 포함된 IPv4 주소를 기반으로 자동터널 생성이 가능하다. 즉 6to4 기술은 터널을 구성함에 있어서 관리자의 관여가 필요하지 않다는 이점이 있다.[6] [8]

3.3 DSTM

'DSTM'은 Pv4 네트워크에서 IPv6 네트워크로

의 전환 과정에서, IPv6 네트워크 내의 듀얼스택 호스트에 IPv6 주소만 할당되고 IPv4 주소는 할당되지 않은 상태로 IPv4 호스트와 통신을 하거나 IPv4 어플리케이션을 실행시켜야 할 필요성을 해결하기 위하여 제시된 기술로서 "Internet-Draft Dual Stack IPv6 Dominant Transition Mechanism" 문서에서 IPv6 전환기술 중 하나로써 정의되고 있는 DSTM 기술은 통신하는 동안 임시 글로벌 IPv4 주소를 동적으로 제공하며, 생성된 동적 터널을 이용하여 IPv6 네트워크에서 IPv6 프로토콜로 캡슐화 된 IPv4 패킷을 전송한다.

즉, IPv6 전용 호스트와 통신할 경우에는 IPv6 스택을 이용하고, IPv4 전용 호스트와 통신할 경우에는 IPv4-in-IPv6 터널링 기술을 이용하여 IPv4 프로토콜 스택을 이용하여 통신하게 된다. 이러한 특성 때문에 DSTM 기술을 사용하는 호스트는 반드시 듀얼스택이어야 하며, IPv6 프로토콜 스택만 있는 호스트일 경우에는 서비스가 불가능하다. 특히 이와 같은 DSTM 기술을 이용하면 IPv4 프로토콜을 그대로 사용할 수 있기 때문에 IPv6 네트워크에서도 IPv4 전용 어플리케이션을 수정 없이 사용할 수 있다는 장점이 있다.[3]

3.4 ISATAP

'ISATAP'은 "RFC 4214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)" 에 정의되어 있으며 IPv4 네트워크에 있는 듀얼스택 노드가 IPv6 패킷을 자동 터널링하는 기술이다. IPv4 네트워크에서 듀얼스택 호스트와 듀얼스택 라우터의 연결 필요성으로 등장하였으며, IPv4 기반의 인트라넷에서 IPv6 호스트를 설치함으로써 사용이 가능하다.[9],

3.5 Teredo

NAT(Network Address Translator)를 이용한 사설네트워크를 사용하고 있는 많은 SOHO(Small office/Home office)와 IPv6 네트워크 간 통신을 지원하기 위하여 일반적으로 캡슐화 방법을 사용한다. Dual Stack 호스트가 생성한 IPv6 패킷을 IPv4 프로토콜로 캡슐화할 때 프로토콜 41번을 사용하게 되는데, NAT는 일반적으로 이러한 작업을 수행하지 못한다. 이러한 NAT 내부의 사설 네트워크에서 UDP 프로토콜을 이용하여 IPv6 프로토콜을 사용할 수 있도록 Teredo 기술이 제시되었다. 표준문서 "RFC4380: Teredo-Tunneling IPv6 over UDP through Network Address Translations (NATs)" 에 IPv6 전환기술 중 하나로써 정의되어 있는 Teredo 기술은 NAT 내부에서 사설 IP를 사용하는 듀얼스택 호스트가 IPv6 전용 호스트와의 통신을 위해 자동 터널을 설정하여 통신이 가능하도록 지원하며, 서로 다른 NAT 네트워크에서 사설 IP를 이용하는 듀얼스택 호스트 간의 통신도 지원한다.[4] [5]

3.6 Tunnel Broker

터널 브로커(Tunnel Broker)는 IPv6 in IPv4 터널의 설정을 제공하는 웹 기반 툴로서 사용자가 웹 서버에 접속하면 우선 적절한 사용자 인증 및 허가 등의 사용자 접근제어를 거친 뒤 간단한 스크립트를 반환함으로서 이를 실행한 사용자 단말이 터널 브로커 서버로 IPv6 in IPv4 터널을 자동 설정하게 한다.[10] 이처럼 터널 브로커는 글로벌 IPv4 주소를 가졌지만 IPv6 망에 대한 직접적인 접속을 가지지 못한 듀얼스택 노드에게 간단한 방식으로 IPv6 접속을 제공받을 수 있게 한다. 이를 이용한 대표적인 서비스의 예로 freenet6 가있다.

IV. 보안 위협 분석

4.1 DSTM

DSTM에서 발생할 수 있는 공격 유형으로는 DNS 서버를 가장한 공격, 클라이언트를 가장한 공격, TEP을 가장한 공격, DSTM 서버를 가장한 공격, 소스 스푸핑 등이 있다. 공격자는 DNS 서버를 가장하여 잘못된 응답을 전송함으로써 IPv6 노드가 보내는 패킷을 IPv4상의 특정 노드로 보낼 수 있으며 DSTM 클라이언트로 가장한 공격자는 다량의 DHCP 요청을 발생함으로써 DHCPv6 서버의 과부하를 초래하고 관리 중인 주소 Pool의 오버플로우로 인한 정상적인 질의/응답 처리를 방해할 수 있다.[11]

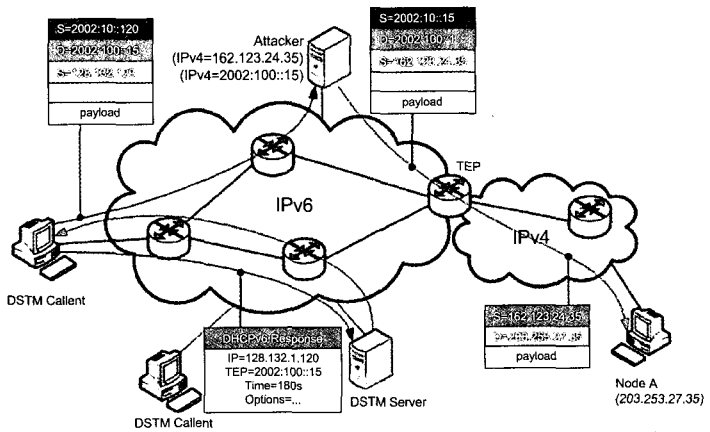
공격자가 TEP을 가장하는 경우 DSTM 클라이언트간의 통신을 방해하고 패킷의 내용을 변경할 수 있다.

DSTM 서버를 가장한 공격자는 클라이언트의 DHCPv6 질의에 대한 응답으로 공격자의 IPv6 주소를 TEP에 지정하여 전송한다. 응답을 수신한 클라이언트는 IPv4 헤더의 소스 주소에 자신의 IPv4 주소를 지정하고, 패킷에 지정된 TEP의 IPv6 주소로 패킷을 전송한다(패킷이 공격자로전달됨). 이때 패킷을 수신한 공격자는 클라이언트의 패킷을 가로채어 임의의 곳으로 전송하거나 내용을 변경할 수 있다. 공격자는 패킷 내부의 IPv4 주소를 자신의 IPv4 주소로 변경하여 TEP으로 전송한다. Node A로 부터의 수신패킷은 TEP을 경유하여 공격자로 전송되며, 공격자는 IPv4 목적지 주소를 DSTM 클라이언트의 IPv4로 변경하여 DSTM 클라이언트로 전송한다. 결국 DSTM 클라이언트와 Node A간의 모든 트래픽은 항상 공격자를 경유하게 된다.[11]

4.2 Teredo

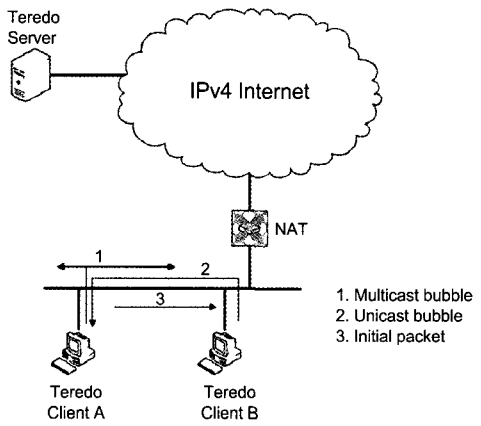
Teredo에서는 릴레이와 서버를 가장한 DoS 공격, 캐쉬 오버플로우를 이용한 DoS 공격, 로컬 Peer 발견 절차에 대한 DoS 공격 등이 발생할 수 있다.

악의적인 릴레이를 Teredo 서비스의 IPv6 측에 설치하고 잘못된 Teredo IPv6 Prefix를 광고하도록 함으로써 라우팅 DoS 공격을 감할 수 있다. Teredo 클라이언트는 최근에 통신한 상대방의 정보를 캐쉬



(그림 2) DSTM 서버와 TEP을 가장한 공격자에 의한 MITM 공격

에 저장하는데, 만일 공격자가 여러 peer로 가장하여 다량의 패킷을 보내는 경우 클라이언트의 캐쉬에 오버플로우가 발생할 수 있다.[11]



(그림 3) 로컬 Peer 발견 절차

정상적인 경우 Teredo 클라이언트 A는 Teredo IPv4 Discovery 주소(IPv4 멀티캐스트)로 버블 패킷을 보내면(on-link 주소, 포트인지 검사) 패킷 수신 후 클라이언트 B는 유니캐스트 주소를 지정해서 클라이언트 A로 응답한다.

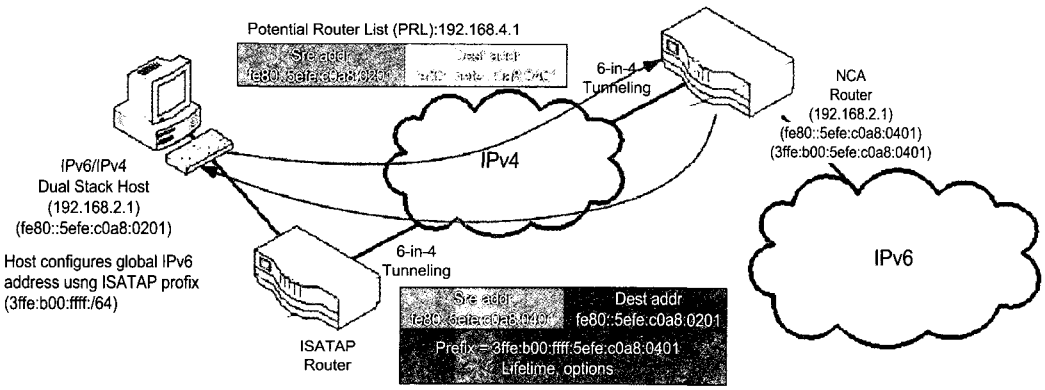
Teredo 클라이언트 A가 공격자인 경우 로컬 링크에 존재하는 Teredo 클라이언트에 대한 유니캐스트 주소를 획득함(로컬 망의 토폴로지 유출)으로써 유니캐스트 주소를 이용해 DoS/MITM 공격을 감행할 수 있다.

Teredo 클라이언트 B가 공격자인 경우 Teredo 발견 요청 메시지에 대해 spoofed된 Teredo 유니캐스트 응답 메시지를 보내고 Teredo 클라이언트 A는 악의적인 노드의 정보를 저장하게 된다. 이때 격자 B가 다량의 응답 패킷을 위조해서 Teredo 클라이언트 A로 보내는 경우 A는 이 정보를 캐쉬에 저장하게 되어 오버플로우가 발생한다.

4.3 ISATAP

ISATAP 보안 위협은 크게 ISATAP 링크 내부에 존재하는 라우터를 가장한 공격자에 의해 패킷 가로채기가 가능하도록 하는 PRL(Potential Router List) 공격, IPv6 주소 구성 과정에 공격자가 개입하여 잘못된 주소를 제공함으로써 DoS 공격, IPv6 주소 구성 과정에 공격자가 개입하여 잘못된 주소를 제공함으로써 MITM 공격이 있다.[11]

ISATAP 라우터는 호스트의 요청(Solicitation)에 의해 IPv6 프리픽스 주소를 광고할 수 있고 이를 수신한 ISATAP노드는 자신의 IPv4 주소를 포함한



(그림 4) ISATA 프리픽스 광고 절차

글로벌 IPv6 주소를 생성한다.[9]

그러나 인증되지 않은 ISATAP 라우터로부터의 프리픽스를 허용하는 경우 잘못된 주소를 생성하여 트래픽 전송이 불가능하거나 공격자가 지정한 임의의 위치로 보내지게 된다.

공격자는 PRL(Potential Router List) 공격을 통해 자신의 주소를 ISATAP 호스트의 PRL에 등록한다. 호스트는 주소 구성을 위해 ISATAP 프리픽스를 요청하는데 이때 등록된 PRL 리스트에서 라우터를 선택한다. 이때 만일 공격자에 의해 설치된 라우터가 선택되는 경우 요청 패킷은 공격자 라우터로 전송되고 공격자는 패킷을 변경하여 정상적인 라우터로 프리픽스를 요청하게 된다. 정상 라우터로부터 수신된 프리픽스 응답을 수신한 공격 라우터는 프리픽스 내용을 수정하여 ISATAP 호스트로 응답하며 이후의 모든 패킷은 공격자를 경유하여 송수신된다.

4.4 6to4

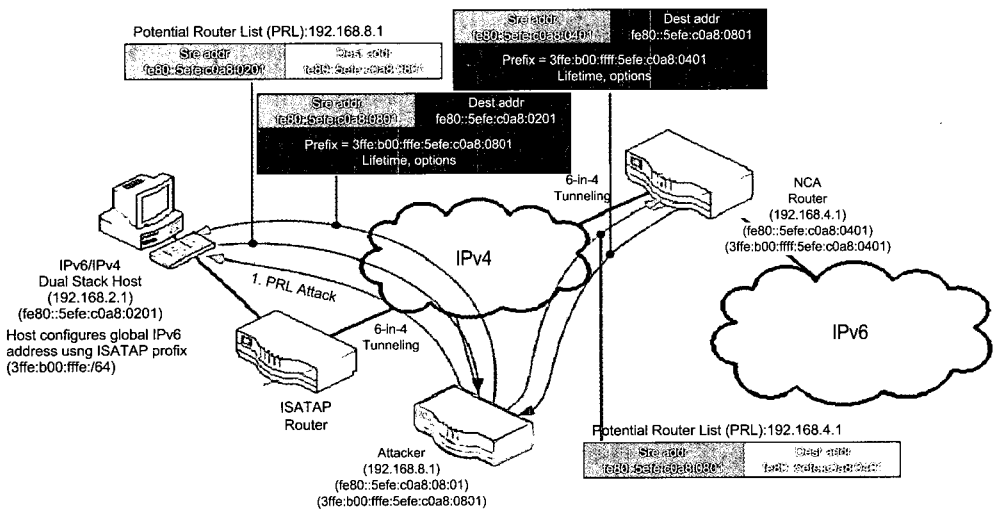
6to4 보안 위협은 로컬 브로드캐스트를 이용한 DoS 공격, Pv6 소스 주소 스푸핑을 이용한 임의의 노드(IPv6 또는 6to4 호스트)에 대한 공격이 있다.

공격자는 공격 대상 노드를 소스 주소로 위조하여 패킷을 전송한다. 6to4 라우터 1은 IPv4 헤더를 추가하여 IPv4 망으로 전송하고 목적지의 6to4 라우터 2는 IPv4 헤더를 제거한 뒤 IPv6 목적지 노드로 패킷을 전송한다. 이때, IPv6는 정상적인 처리과정을 통해 6to4 라우터2로 응답 패킷을 보내는데 6to4 라우터2는 IPv4 헤더를 추가하여 IPv4 망으로 패킷을 터널링 하게 되고 6to4 라우터1은 IPv4 헤더를 제거한 후 패킷을 희상 노드로 전송한다.[11]

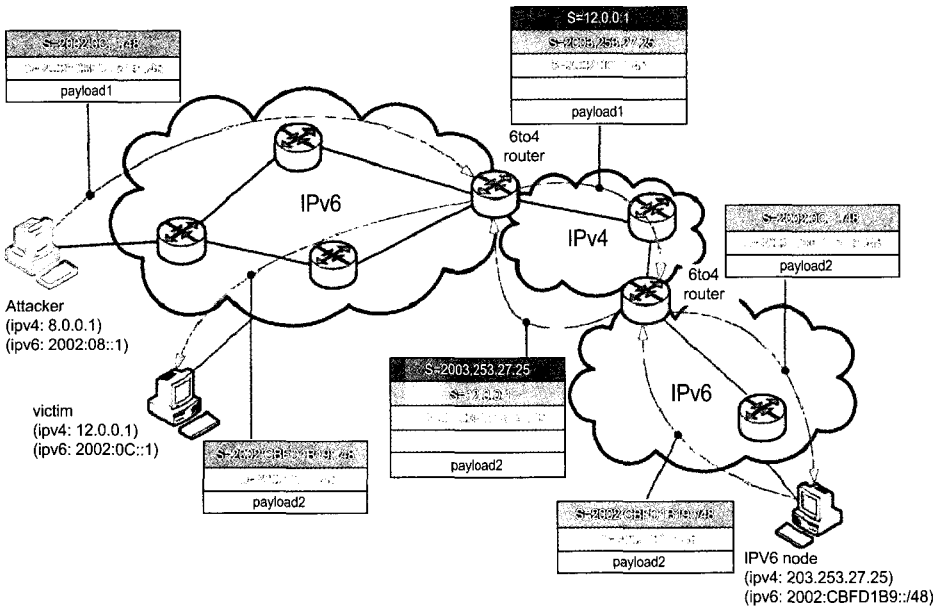
4.5 터널 브로커

터널 브로커 보안 위협으로는 터널 서버를 가장한 DoS 공격, DNS를 가장한 DoS 공격, 터널 브로커를 가장한 DoS및 MITM 공격, 터널 브로커를 대상으로 하는 DoS 공격등이 있다.

공격자가 터널 브로커를 가장하는 경우 듀얼 스택 클라이언트 노드, DNS 서버, 터널 브로커에 대한 광



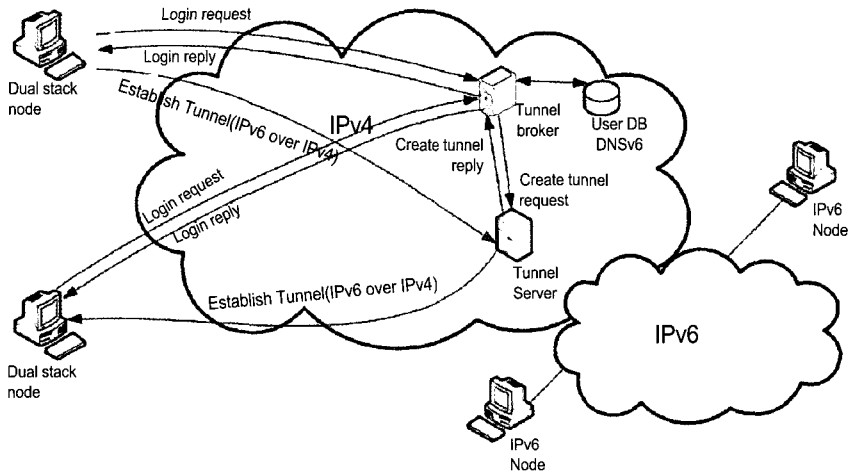
(그림 5) 라우터를 가장한 공격자에 의한 MITM 공격



(그림 6) IPv6 소스 주소 스푸핑 공격

범위한 공격이 가능하다.[11] 절차는 다음과 같다.

듀얼 스택 노드는 터널 브로커로 로긴 요청을 보내면 터널 브로커는 듀얼스택 클라이언트로부터의 요청을 거부함으로써 DoS 공격을 발생시킨다. 이때 터널 브로커는 터널 서버로 다량의 터널 생성 요청을 보냄으로써 터널 서버에 대한 자원 고갈을 발생시킬 수 있고 터널 브로커는 DNS 서버로 다량의 주소 해석 요청을 보냄으로서 서버 자원의 고갈을 발생시키고 정상적인 브로커로부터의 주소 해석을 방해할 수 있다.[2]



(그림 7) 터널 브로커에 의한 공격

4.6 6in4

6in4에서의 보안 위협은 소스 주소 Spoofing을 이용한 공격, 6in4라우터를 가장한 공격자에 의한 패킷 Sniffing 공격, 6in4 라우터에 의한 MITM 공격이 있다.

6in4의 IPv6 주소는 96비트의 '0'과 32비트의 IPv4 주소로 구성되는데, 공격자가 IPv6 패킷 전송 시 패킷 내부의 IPv4 주소를 위조함으로서 응답 패킷은 임의의 노드로 전송될 수 있다.[5,6,11]

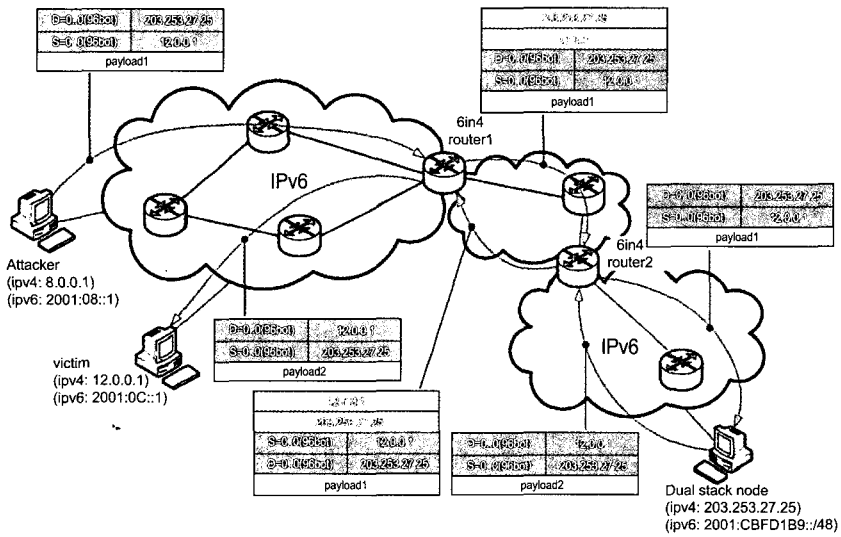
공격자는 희생 노드의 IPv4 주소를 소스 주소로 지정하여 패킷을 6in4 라우터로 전송하고 6in4 라우터1은 IPv6 주소를 참조하여 패킷의 외부를 IPv4로 캡슐화한 후 IPv4 망으로 전송한다.

이때 패킷을 수신한 6in4 라우터 2는 패킷에서 IPv4 헤더를 제거한 후 목적지 노드로 전송하며 목적지 노드는 수신 패킷에 대한 응답 패킷을 6in4 라우터 2로 전송한다. 6in4 라우터 2는 수신된 패킷을 참조하여 IPv6 패킷 외부를 IPv4 헤더로 캡슐화 한 후 6in4 라우터 1로 전송하는데 6in4 라우터 1은 수신 패킷에서 IPv4 헤더를 제거한 후 희생 노드로 응답 패킷을 전송한다.

V. 결 론

본 연구에서는 터널링 방식에 초점을 둔 IPv4/IPv6 혼재 네트워크에서의 서비스에 관한 보안 위협을 분석하고 사용가능한 대응 방법을 기술하였다. 네트워크 변환에 있어서의 보안 문제점은 '패킷 가로채기', '부적절한 네트워크 동작', '디자인 시 장애 감내 기능 결여' 등의 요인으로 파악할 수 있다.[12]

패킷 가로채기 공격은 RA(Router Advertisement)나 DHCP 서버를 가장한 공격, 방화벽에 의한 ICMP 패킷 필터링 등이 있고, 부적절한 네트워크 동작 요인에는 DNS 서버 응답 취약점, 터널링 관리 오류 등이 있다. 디자인 시 장애 감내 기능 결여에 따른 요인으로는 잘못된 TCP 오류 응답, DNS를 통한 잘



(그림 8) IPv4 소스 주소 스푸핑에 의한 공격

못된 IPv6 주소 획득 등이 존재한다. IPv4/IPv6 혼재 네트워크에서의 보안 제공은 순수 IPv4 네트워크 또는 IPv6 네트워크에서의 보안보다 더 복잡하고 어려운데 이는 IPv4 네트워크와 IPv6 네트워크 어느 한 곳에 대한 보안을 완벽히 제공해도 다른 쪽의 위협 노출로 인해 전체적인 보안이 향상되지 않기 때문이다.

변환 방법들은 프로토콜 자체적으로 또는 듀얼 스택 사용을 통해 IPv4 네트워크와 IPv6 네트워크에 동시에 노출되며 각 요소들이 공격의 대상이 될 수 있다. 따라서 IPv4/IPv6 혼재 네트워크를 공격자로부터 안전하게 격리하기 위해서는 IPv4 네트워크와 IPv6 네트워크 자체에 대한 보안 위협 제거가 우선되어야 하며 기존 서비스 엔티티 간의 강력한 SA 설정이 보장되어야 한다.[11] [12]

[참 고 문 헌]

[1] S. Deering and R. Hinden, RFC 2460: Internet Protocol, Version 6 (IPv6), Dec. 1998.

[2] 한국정보보호진흥원, IPv6 보안 기술 해설서, Oct. 2005.

[3] J. Bound, L. Toutain, and JL. Richier, Internet-Draft: Dual Stack IPv6 Dominant Transition Mechanism, Oct. 2005.

[4] 한국전산원, "IPv6 in IPv4 터널링 기술 현황".

[5] P. Savola, Internet-Draft: Firewalling Considerations for IPv6, Oct. 2003.

[6] E. Nordmark and R. Gilligan, RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers, Oct. 2005.

[7] 한국전산원, "IPv4/IPv6 전환 실무자 지침서".

[8] R. Gilligan and E. Nordmark, RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers, Aug. 2000.

[9] F. Templin, T. Glesson, M. Talwar, and D. Thaler, RFC 4214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Oct. 2005.

[10] A. Durand, P. Fasano, I. Gaurdini, and D. Lento, RFC 3053: IPv6 Tunnel Broker, Jan. 2001.

[11] E.Davies, S.Krishnan, P.Savola, Internet-Draft: IPv6 Transition/CO-existence Security Considerations, Jul. 2005.

[12] P. Savola and C. Patel, RFC 3964: Security Considerations for 6to4, Dec. 2004.

김미영

1992년 전주우석대학교 졸업(학사)
1995년 광운대학교 대학원 전산학과 졸업(석사)
1995년~1997년 (주)필컴 시스템 개발부 근무
2000년 ~ 2005년 숭실대학교 대학원 컴퓨터학과 졸업(박사)
2005년 ~ 현재 숭실대학교 정보미디어 연구소 전임연구원
관심분야 : IPv6, Mobile IP, AAA, Network Security

문영성

1993년 연세대학교 전자공학과(학사)
1986년 Univ. of Alberta 전자공학과 졸없(석사)
1993년 Univ. of Texas, Arlington 전산학과 졸업(박사)
1994년 ~ 현재 숭실대학교 컴퓨터학부 교수
관심분야 : Mobile IP, Security, IPv6, Grid