보안취약점 테스트를 위한 IPv4/IPv6 혼재 네트워크 구축 방법

김정욱*, 문길종*, 김용민**, 노봉남***

*전남대학교 정보보호협동과정, **전남대학교 전자상거래전공, ***전남대학교 전자컴퓨터정보학부

A Implementation Method of mixed IPv4/IPv6 Network for Testing Security Vulnerability

Jeong-Wook Kim*, Gil-Jong Mun*, Yong-Min Kim**, Bong-Nam Noh***

*Interdisciplinary Program of Information Security, Chonnam National University, **Dept. of Electronic Commerce, Chonnam National University, ***Div. of Electronics, Computer and Information Eng., Chonnam National University

요 약

IPv6는 IPv4의 주소 부족을 해결하기 위해 1998년 IETF에서 표준화된 프로토콜이다. 현재 IPv4가 주축으로 되어 있는 인터넷을 동시에 IPv6로 전환하는 것은 불가능하므로 IPv4/IPv6 혼재네트워크를 거쳐 IPv6 순수 망으로 전환될 것이다. 본 논문에 서는 혼재 네트워크에서 IPv4 망과 IPv6 망간의 통신을 가능하게 해주는 IPv6 전환 메커니즘 중 터널링 방식에 대해 기술하고, 보안 취약성을 테스트하기 위해 동일한 보안 취약성에 대해 각각 IPv4 패킷, IPv6 패킷, 터널링된 패킷을 캡쳐할 수 있는 구축방안을 제안한다. 제안된 방식은 IPv4, IPv6, 터널링 패킷에 대한 분석이 가능하므로 IPv6 지원을 계획하는 침입탐지, 침입차단 시스템에 활용이 가능하다.

Ⅰ. 서론

현재 사용하고 있는 IPv4 주소체계는 32비트 주소 체계이므로 이론적으로 2^{32}개(약 43억 개)의 주소를 만들 수 있다. 그러나 클래스 개념의 주소 할당 방법을 사용함으로 인해 비효율적으로 사용되고 있다. 이는 초기 IP 주소 설계 시 수요를 충분히 예측하지 못한 이유에서 비롯되었다. IPv4 주소는 초기의 비효율적인 주소 할당과 인터넷의 급격한 발달 및 첨단 인프라에 따른 고도의 디지털 서비스 지원을 위한 주소 수요의 급증으로 한계점에 근접하고 있다. 이러한 주소부족 문제를 해결하기 위한 임시적인 해결책으로 기존 IPv4 주소 공간을 효율적으로 재구성하는 CIDR(Classless Inter-Domain Routing), NAT (Network Address Translation), DHCP(Dynamic Host Configuration Protocol) 등을 이용한 방식이 있다. 하지만 궁극적으로 주소 고갈을 막는 해결책이 되지 않으므로 인터넷 주소 제공 및 관리를 위한 근본적인 해결을 위해 IETF(Internet Engineering Task Force)는 1998년 128비트의 주소 공간을 갖는 차세대 인터넷 프로토콜인 IPv6를 표준화 하였다. 그러나 IPv6는 IPv4와 호환되지 않고 이미 전 세계적으로 IPv4에 기반을 두고 인터넷이 운영되고 있어 모든 IPv4 네트워크가 IPv6 네트워크로 전환되기 전까지 IPv4/IPv6 혼재네트워크가 전 세계적으로 사용될 것이다. 그리고 이러한 혼재네트워크 환경에 적용할 수 있는 다양한 연동기술들이 개발되었다.

본 논문은 IPv4 망과 IPv6 망 사이의 통신을 지원하는 기술들 중 터널링 방식에 대해서 2장에서 기술하고, 터널링 방식의 구축 방법 및 IPv4/IPv6 혼재네트워크 망에 대해서 3장에서 기술하였으며, 4장에서 결론 및 향후 연구에 대해 기술한다.

Ⅱ. 관련연구

지금까지 학계와 산업계에서 연구된 IPv4/IPv6 혼재네트워크에서 사용할 수 있는 전환기술로는 Dual Stack, Tunneling(6in4, 6to4, ISATAP, DSTM, Teredo, Tunnel Broker), Translation(SIIT, NAT-PT, BIS, BIA, TRT, SOCKs, SQUID) 기술이 있다. 이러한 기술들은 다양한 사용자의 컴퓨팅 환경과 요구사항을 충족시키기 위하여 제안 및 개발되었고, 이 중 IPSec을 지원하는 전환기술은 Dual Stack과 Tunneling 기술이다. 보안이 강화된 IPv6의 특징을 볼 때, IPSec을 지원하는 방식이 주류가 될 것이므로 터널링 기술 중 혼재네트워크 망 구축에 이용된

* 본 연구는 정보통신부 대학 IT 연구센터 육성, 지원사업의 연구결과로 수행되었습니다.

6in4, 6to4, ISATAP, DSTM, Teredo에 대해서 기술한다.

2.1 6in4

6in4는 IPv4망을 통한 IPv6 패킷의 통신을 위해 등장하게 되었고, 기존의 IPv4 인프라를 활용해 IPv6 트래픽을 전송하는 기술이다. 6in4[2]는 IPv4 라우팅 인프라를 통해 전송되도록 IPv6 패킷을 IPv4 헤더 내에 캡슐화 함으로써 이루어지는 터널링 방식이다. 이 기술은 IPv4 주소를 바탕으로 관리자가 터널의 양 끝의 주소를 수동으로 설정하는 방식을 주로 사용한다. 그림 1은 수동 터널링 방식의 패킷형식이다.

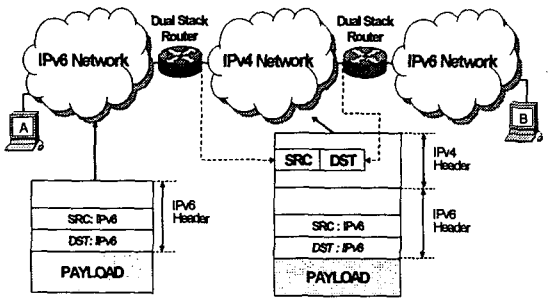

그림 1: 수동 터널링 방식의 패킷형식

2.2 6to4

6to4[3]는 IPv4에서 IPv6 네트워크로의 전환 과정에서 IPv6 프로토콜을 지원하지 않는 IPv4 네트워크 내에 고립된 IPv6 네트워크나 호스트들이 IPv4 네트워크를 이용한 통신을 위해 제시되었다. 6to4 기술은 '2002::/16'의 고유한 라우팅 프리픽스로 시작하는 6to4 주소에 포함된 IPv4 주소를 기반으로 자동터널을 생성한다. 즉, 6to4 기술은 터널을 구성함에 있어서 관리자의 관여가 필요하지 않다는 장점이 있다. 하지만 6to4를 사용하는 IPv6 망과 전형적인 IPv6 망 사이에 통신을 가능하게 하기 위해서는 두 망을 연결해 주는 릴레이 라우터가 존재해야 하고, 6to4 라우터와 릴레이 라우터 사이에 터널이 설정되어 있어야 한다. 그림 2는 자동 터널링 방식의 패킷형식이다.

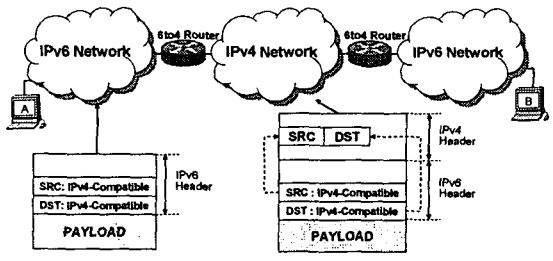

그림 2: 자동 터널링 방식의 패킷형식

2.3 ISATAP

ISATAP[4]은 IPv4 망에서 듀얼 스택 호스트와 라우터의 연결을 위해 제시되었다. IPv4 망에 있는 듀얼 스택 노드가 IPv4 인프라를 통해 IPv6 메시지 자동 터널링하는 기술이다. ISATAP은 64비트의 프리픽스 부분을 전형적인 IPv6 주소와 같은 프리픽스를 사용하고, 그 뒤 32비트는 수정된 EUI-64 방식의 '0000:5eef'를 마지막 32비트는 IPv6 주소 인터페이스 식별자로 IPv4 주소를 사용한다. ISATAP은 IPv4 기반의 인트라넷의 IPv6 호스트에 설치됨으로써 사용이 가능하다.

2.4 DSTM

DSTM[5]은 IPv4에서 IPv6 네트워크로의 전환 과정에서, IPv6 네트워크 내의 IPv6 주소만을 가진 듀얼스택 호스트가 IPv4 호스트와 통신을 하거나 IPv4 어플리케이션의 실행을 위해 제시되었다. DSTM 기술은 통신하는 동안 임시 글로벌 IPv4 주소를 동적으로 DSTM 호스트에 할당하고, 생성된 동적 터널을 이용하여 IPv6 네트워크에서 IPv6 헤더로 캡슐화된 IPv4 패킷을 전송한다. 즉, IPv6 전용 호스트와 통신할 경우에는 IPv6 스택을 이용하고, IPv4 전용 호스트와 통신할 경우에는 IPv4 패킷을 IPv6 헤더로 캡슐화하여 통신하게 된다. 이러한 특징 때문에 DSTM 기술을 사용하는 호스트는 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.

2.5 Teredo

Teredo[6]는 NAT를 이용한 사설 네트워크를 사용하고 있는 많은 SOHO(Small office/Home office)와 IPv6 네트워크 간 통신을 지원하기 위해 일반적으로 캡슐화 방법을 사용한다. 호스트가 생성한 IPv6 패킷을 IPv4 헤더로 캡슐화 할 때, IPv6 헤더의 프로토콜 속성이 41번으로 설정된다. NAT는 일반적으로 이러한 작업을 수행하지 못한다. 이런 이유로 6to4 기술은 공인 IPv4 주소를 필요로 하며, 공인 IPv4 주소가 없는 NAT 환경에서는 IPv6 네트워크와 통신에 어려움이 있다. Teredo는 이러한 NAT 내부의 사설 네트워크에서 UDP 프로토콜을 이용하여 IPv6 프로토콜을 사용할 수 있도록 제시되었다. Teredo는 NAT 내부에서 사설 IP를 사용하는 듀얼스택 호스트가 IPv6 전용 호스트와 통신을 위해 자동 터널을 설정하여 통신이 가능하도록 지원하고, 서로 다른 NAT 네트워크에서 사설 IP를 이용하는 듀얼스택 호스트 간의 통신도 지원한다.

III. 혼재네트워크 망 구축

이번 장에서는 II장에서 설명한 터널링 방식 중에서 6in4와 ISATAP을 이용하여 IPv6 네트워크와 IPv4 네트워크 내에 고립된 IPv6 네트워크와 IPv6 호스트를 연결하고, IPv4/IPv6 혼재네트워크 망을 구축하는 방법에 대해서 설명한다.

3.1 6in4

6in4 망을 구축하기 위해서는 관리자가 터널의 양 끝에서 수동으로 터널링을 설정해 주어야한다. 외부 네트워크와 연결하기위해 한국전산원으로부터 IPv6 주소를 할당 받고, 한국전산원의 라우터와 터널링을 수동으로 맺음으로써 6in4 망을 구축할 수 있다. 라우터는 RADVD[7]를 이용하여 서브네트워크에 RA (Router Advertisement) 메시지를 전송한다. /etc/radvd.conf 파일에서 RA 메시지를 통해 전송할 정보들을 수정한다.

```
interface eth1
{
  AdSendAdvert on;
  UnicastOnly on;
  MinRtrAdvInterval 30;
  MaxRtrAdvInterval 100;
  AdvHomeAgentFlag off;
  prefix 2001:2b8:2:3100::/64
  {
  AdvOnLink on;
  AdvAutonomous on;
  AdvRouterAddr off;
  AdvValidLifetime 300;
  AdvPreferredLifetime 120;
  };
};
```

호스트는 IPv6 스택만 설치되어 있다면 특별한 설정 없이 라우터로부터 프리픽스를 할당 받아 자동으로 주소를 구성해 통신할 수 있다.

6in4, 6to4 터널의 생성 및 활성화 명령어이다.

```
# ip tunnel add 터널 인터페이스 명 mode sit
  remote IPv4 주소 local IPv4 주소 ttl 255
# ip link set 터널 인터페이스 명 up
```

6in4 패킷은 프로토콜 41번을 사용하므로 패킷 허용을 위해 내부 방화벽 설정을 해줘야한다.

```
### Accept IPv6-in-IPv4 Packet
iptables INPUT -p 41 -j Accept
iptables -I FORWARD -p 41 -j ACCEPT
iptables -I OUTPUT -p 41 -j ACCEPT
```

3.2 ISATAP

ISATAP 망을 구축하기 위해서는 리눅스 커널 2.4.21(USAGI)[8]을 이용해 커널 컴파일을 하거나 usagi-linux24-stable 패치 파일을 다운받은 후, 커널을 패치해야 한다. 그림 3과 같이 커널 컴파일 옵션 중, 네트워크 옵션에서 'IPv6 : ISATAP interface support' 을 선택하고, 커널 컴파일을하고, 터널 생성 후 활성화하면 ISATAP 터널링을 이용할 수 있다. ISATAP 터널링은 네트워크 간에 터널링을 할 수 없기 때문에 네트워크 간 터널링은 6in4나 6to4 등의 다른 터널링 방식을 이용하여 외부와 통신을 맺을 수 있다.

```
[*] TCP/IP networking
[ ]   The IPsec protocol (EXPERIMENTAL)
[*]   IP: multicasting
[ ]   IP: advanced router
[ ]   IP: kernel level autoconfiguration
< >   IP: tunneling
< >   IP: GRE tunnels over IP
[ ]   IP: multicast routing
[ ]   IP: ARP daemon support (EXPERIMENTAL)
[ ]   IP: TCP Explicit Congestion Notification support
[ ]   IP: TCP syncookie support (disabled per default)
<M>   The IPv6 protocol (EXPERIMENTAL)
[ ]     IPv6: verbose debugging messages
[ ]     IPv6: inter-module support.
[ ]     IPv6: drop packets with fake ipv4-mapped address(es)
[ ]     IPv6: 6to4-address in nexthop support.
[ ]     IPv6: Privacy Extensions (RFC 3041) support
[ ]     IPv6: anycast support
[*]     IPv6: ISATAP interface support (EXPERIMENTAL)
[ ]     IPv6: sub-tree in routing table support (just for testing)
[ ]     IPv6: disable optimization MLD6 Done message
[ ]     IPv6: enable Node Information Queries
< >     IPv6: IPv6 over IPv6 Tunneling (EXPERIMENTAL)
```

그림 3: 커널 컴파일 시 선택 사항

ISATAP 라우터 터널 생성 및 활성화 명령어이다.

```
# ip tunnel add is0 mode isatap local <IPv4 주
  소> ttl 255
# ip link set 터널 인터페이스 명 up
```

리눅스 기반 ISATAP 호스트의 터널 생성 및 활성화 명령어이다.

```
# ip tunnel add is0 mode isatap local <IPv4 주
  소> v4any <isatap 라우터 IPv4 주소> ttl 255
# ip link set 터널 인터페이스 명 up
```

윈도우 XP 기반 ISATAP 호스트의 IPv6 스택 설치, 터널 생성 및 활성화 명령어이다.

```
C:\>netsh interface ipv6 install
C:\>netsh interface ipv6 isatap set router<isatap 라
    우터 IPv4 주소> enabled
C:\>netsh interface isatap set state enabled
```

3.3 혼재네트워크 망 및 테스트

그림 6은 지금까지 설명한 터널링 방법을 이용하여 고립된 IPv6 네트워크끼리의 연결과 IPv4 네트워크 내의 고립된 IPv6 호스트와 IPv6 네트워크와의 연결을 통한 IPv4/IPv6 혼재네트워크 망 구성도를 보여준다.

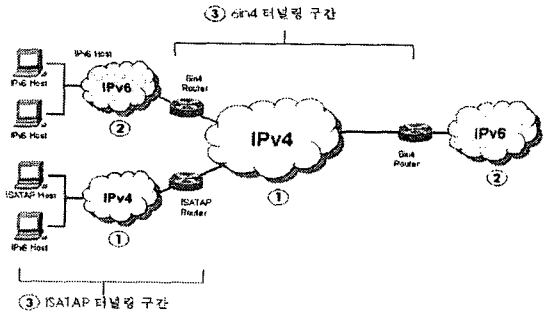

그림 4: IPv4/IPv6 혼재네트워크 구성도

그림 6에서 볼 수 있듯이 ①에서 IPv4 패킷을, ②에서 IPv6 패킷을 캡쳐할 수 있고, ③에서 터널링 패킷을 캡쳐할 수 있다. 따라서 동일한 보안 취약성에 대해 각각 IPv4 패킷, IPv6 패킷, 터널링된 패킷에 대한 분석이 가능하므로, IPv6 지원을 계획하는 침입탐지, 침입차단 시스템에 활용할 수 있다.

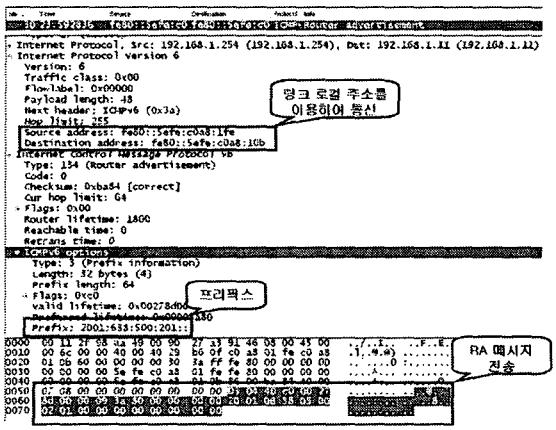

그림 5: RA 메시지 전송

그림 6은 ISATAP 라우터에서 ISATAP 호스트로 RA 메시지를 전송한 것이다. RA 메시지는 ISATAP 라우터와 호스트의 IPv6 링크로컬 주소로 통신을 하고, 이 IPv6 패킷은 ISATAP 라우터와 호스트의 IPv4 주소를 송신지와 목적지 주소로 갖는 IPv4 헤더로 캡슐화되어 통신한다. ISATAP 호스트는 라우터로부터 받은 RA 메시지를 통해 프리픽스를 할당받고, IPv6 주소를 구성한다.

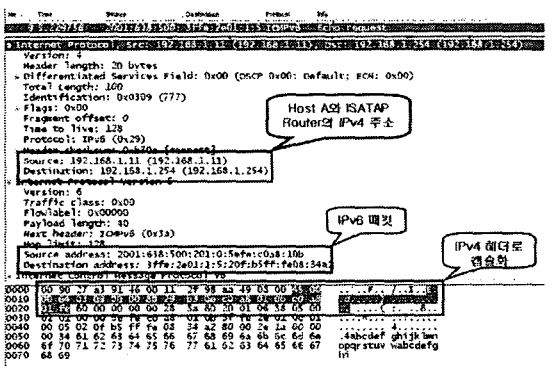

그림 6: 터널링 패킷

그림 7은 혼재네트워크 망을 구축한 후 ISATAP 호스트에서 IPv6 네트워크의 호스트까지 통신을 한 것이다. ISATAP 호스트는 IPv6 패킷을 자신의 IPv4 주소와 ISATAP 라우터의 IPv4 주소를 송신지와 목적지 주소로 갖는 IPv4 헤더로 캡슐화하여 ISATAP 라우터까지 전송하고 이 캡슐화된 패킷은 6in4 라우터에서 디캡슐화되어 IPv6 패킷으로 목적지 IPv6 네트워크 호스트까지 전송한다.

Ⅳ. 결론

본 논문에서는 IPv4/IPv6 혼재네트워크에서 사용할 수 있는 일반적인 기술들 중에서 6in4, 6to4, ISATAP, DSTM Teredo 터널링 방식에 대해 설명하고, IPv4/IPv6 혼재네트워크 망을 구축하기위해 터널링 구축 방법에 대해서 설명하였다. 그리고 구축된 IPv4/IPv6 혼재네트워크 망이 침입탐지, 침입차단 시스템에서의 활용을 위한 IPv4, IPv6, 터널링 패킷에 대한 분석이 가능함을 보이고, 정상적인 통신이 이루어지고 있음을 확인하였다.

향후에는 구축된 환경에서 각각의 터널링 방식이 가지는 보안 취약점에 대한 연구와 함께 IPv4/IPv6 혼재네트워크에서 발생 가능한 새로운 보안 취약점을 찾고 이를 해결하기 위한 해결 방안을 제시할 것이다.

[참고문헌]

[1] S.Deering and R.Hinden, Internet Protocol, Version 6 Specification, RFC 2460, IETF, December, 1998

[2] E. Nordmark and R.Gilligan, Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213, IETF, October, 2005

[3] B. Carpenter and K. Moore, Connection of IPv6 Domains via IPv4 Clouds, RFC 3056, IETF, February, 2001

[4] F. Templin, T. Gleeson, M. Talwar and D. Thaler, Intra-Site Automatic Tunnel Addressing Protocol, RFC 4214, IETF October, 2005

[5] J. Bound, L. Toutain and JL. Richier, Dual Stack IPv6 Dominant Transition Mechanism, draft-bound-dstm-exp-04.txt, IETF, October, 2005

[6]C. Huitema, Teredo: Tunneling IPv6 over UDP through Network Address Translations, RFC 4380, IETF, February, 2006

[7] Litech Systems Design, http://www.litech.org/

[8] USAGI Project, http://www.linux-ipv6.org/