IPv6 전환기술에서의 보안 취약점 분석

윤성열*, 심용훈**, 박석천***
*, **,경원대학교 일반대학원 전자계산학과
***경원대학교 IT대학
e-mail:scpark@kyungwon.ac.kr

Analysis of Security Vulnerability in IPv6 Transition Technology

Sung-Yeol Yun*, Yong-Hoon Sim**, Seok-Cheon Park***
*, ** ,***Division of Computer Science, Kyungwon University

요 약

인터넷의 빠른 발전으로 인한 사용자의 증가와 통신·방송의 융합, 홈네트워크 등의 신규 서비스들은 IPv4의 인터넷 주소 고갈을 증대시켰으며, 더불어 차세대 인터넷 프로토콜인 IPv6의 제정 및 보급과 함께 IPv6 전환기술에서의 보안 취약점이 주요한 화두로 떠오르고 있다. 본 논문에서는 IPv6로의 성공적인 전환 체계를 확립하기 위하여 IPv6 전환기술 및 전환기술에서의 보안 취약점과 대응방안에 대하여 연구한다.

1. 서론

IPv4(Internet Protocol version 4)에 기반한 현재의 인터넷은 사용자의 급속한 증가로 인해 주소고갈 문제에 직면하고 있으며, 새롭게 등장하고 있는 휴대 인터넷 및 통신·방송의 융합, 홈네트워크 등의 신규 서비스들로 인해 인터넷 주소 고갈을 더욱 앞당기고 있다. 인터넷 수요의 증가로 인한 인터넷주소 고갈의 문제가 수면위로 부각되면서 인터넷 주소 부족을 해결할 IPv6(Internet Protocol version 6) 주소체계 도입의 필요성은 그 어느 때보다 강조되고 있다.

실제로 국제인터넷주소할당기관인 IANA(Internet Assigned Numbers Authority)는 IPv4 주소 잔여 공간이 완전히 고갈되어 2011년 2월 4일 글로벌 IPv4 신규 할당 중단을 선포하였다. IETF(Internet Engineering Task Force)는 이러한 주소 부족 문제를 해결하기 위하여 IPv6를 개발하였고 표준화가 완료되어 현재 도입기에 들어서고 있다[1]. IPv6는 기존 IPv4가 지니고 있는 주소부족 문제를 자연스럽게 해결할 수 있으며, 정보보안 및 서비스 품질 보장에 대한 보다 효율적인 기능으로 처리될 수 있는 진보된 형태의 서비스를 가능하게 한다. 하지만, IPv6는 강화된 보안 기능에도 불구하고 많은 보안 취약점들을 가지고 있으며, IPv4와 동일한 보안 취약점뿐만 아니라 새로운 보안 취약점도 존재한다. 따라서 IPv4에서 IPv6로 성공적인 전환을 위해서는 효율적인 보안 관리를 위한 보안 취약점 연구과 대응 방안이 필요하다.

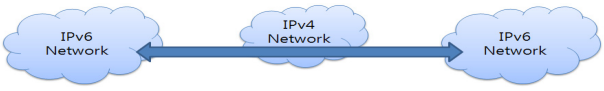
이에 따라 본 논문에서는 21세기 정보화 사회 패러다임의 변화에 따른 서비스 수요의 대안이라고 볼 수 있는 차세대인터넷주소자원의 구축 및 응용 사업의 지속적인 추진을 위하여 IPv4와 IPv6 사이의 연동을 지원하기 위하여 개발된 다양한 IPv6 전환 기술들을 고찰하고 IPv6 전환 기술 환경에서 고려해야 할 차세대 보안 기술 취약점 및 대응방안에 대하여 연구한다.

2. 관련연구

IPv6 전환 기술은 크게 터널링(Tunneling), 듀얼스택(Dual Stack), 변환(Translation) 방식으로 구분할 수 있다.

2.1 IPv4/IPv6 터널링 기술

IPv4 기반 환경에서의 IPv4/IPv6 터널링은 설정 터널링(Configured Tunneling) 방식과 자동 터널링(Automatic Tunneling) 방식으로 구분 할 수 있다[2].



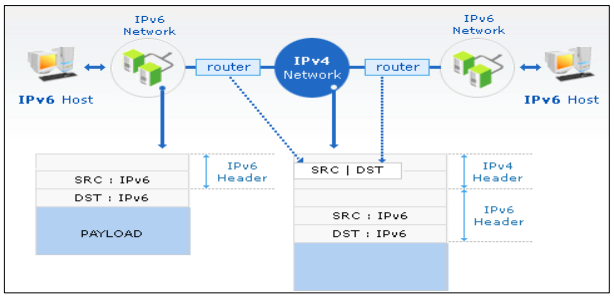
(그림 1) IPv6 터널링 기술

2.1.1 설정 터널링(Configured Tunneling)

설정 터널링은 6Bone에서 주로 사용하는 방법으로 두 라우터 간(혹은 호스트간)의 IPv4 주소를 통해 매뉴얼하

* 경원대학교 일반대학원 전자계산학과 박사과정
** 경원대학교 일반대학원 전자계산학과 석사과정
*** 경원대학교 IT대학 정교수(교신저자)

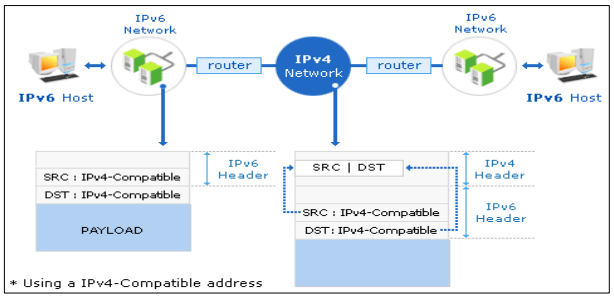
게 정적으로 터널을 설정하는 방식이다. 그림 2는 설정 터널링에 대한 그림이다[3].



(그림 2) 설정 터널링

2.1.2 자동 터널링(Automatic Tunneling)

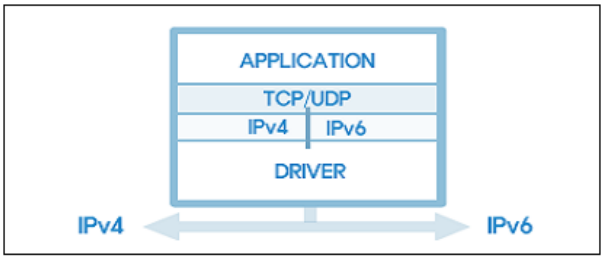
자동 터널링은 IPv4 호환 주소를 이용하여 설정 없이 IPv4 구간을 통과할 때면 IPv4 호환 주소에 내포되어 있는 IPv4 주소를 통해 자동으로 터널링을 해주는 방식으로 최근에는 IPv4 호환 주소를 이용한 자동 터널링 방식보다 6to4, ISATAP과 같은 향상된 자동 터널링 방식을 더 선호한다. 그림 3은 자동 터널링에 대한 그림이다[4].



(그림 3) 자동 터널링

2.2 듀얼스택(Dual Stack)

IPv6 노드가 IPv4 전용 노드와 호환성을 유지하는 가장 쉬운 방법은 IPv4/IPv6 듀얼 스택을 제공하는 것이다. IPv4/IPv6 듀얼 스택 기술은 하나의 시스템에서 IPv4와 IPv6 프로토콜을 동시에 처리하는 기술로써 그림 4처럼 듀일 스택 기술을 지원하는 시스템은 물리적으로 하나의 시스템이지만 논리적으로 IPv4와 IPv6을 지원하는 두 개의 시스템이 있는 것처럼 볼 수 있다[5].



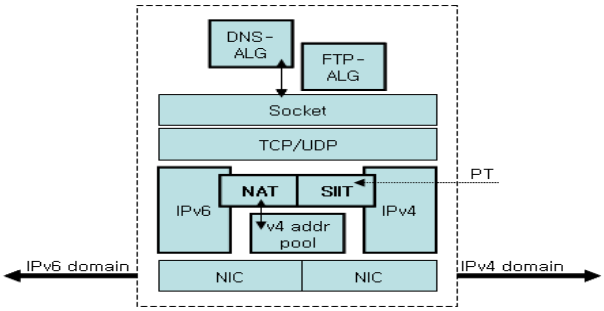
(그림 4) 듀얼스택

2.3 IPv6 변환 기술

IPv4와 IPv6의 헤더 구조 및 길이가 다르기 때문에 IPv4, IPv6 환경에서 통신을 할 때에는 서로에게 맞는 IP 프로토콜 형태로 변환하기 위해 IP 헤더를 변환하는 과정이 필요하다. 이러한 헤더 변환방법으로 NAT-PT, SIIT 등이 있다.

2.3.1 IPv6 변환 기술

NAT-PT는 세션이 초기화될 때마다 동적으로 IPv6 노드에 IPv4를 할당하기 위한 주소 pool을 가지고 두 망간의 경계 라우터에 주로 위치하는 NAT 기능으로 address mapper로서 동작을 한다. 그림 5는 NAT-PT 기본 구조를 보여준다[6].



(그림 5) NAT-PT 기본구조

2.3.2 SIIT(Stateless IP/ICMP Transaction) 변환 기술

전용 IPv6 노드가 IPv4 노드와의 통신이 가능하기 위해서는 중간의 IPv6 패킷을 IPv4 패킷으로 변환하거나 반대로 IPv4 패킷을 IPv6 패킷으로 변환해주는 과정이 필요하다. SIIT는 IP 패킷의 변환을 담당하기 위한 기술로써 IPv6 변환 방법의 개념보다는 IPv6 변환방법을 지원하기 위한 IP 프로토콜 변환 기술 그 자체로 볼 수 있다. 그림 6은 SIIT 변환기술에 대한 그림이다[7].

(그림 6) SIIT 변환기술

3. IPv4/IPv6 전환기술의 보안 취약점 및 대응방안 분석

IPv6 환경으로 전환시 나타날 수 있는 보안 위협은 IPv4에서 존재하였던 위협 요소뿐만 아니라 IPv6에서 새로이 나타날 위협 요소를 포함하여 복합적으로 나타날 수 있다. IPv6 주소공간이 128비트로 확장되어 스캐닝이나 이를 이용하는 웜과 같은 것들은 IPv6에서 대폭 감소될 것으로 예상되고 있다[8]. 하지만, IPv4에서 IPv6로 전환

하는 기술인 터널링, 듀얼 스택, 변환 기술은 보안의 취약점으로 작용할 수 있다. 다음 표 1은 IPv6 적용기술에 따른 보안취약점에 대한 내용이다.

<표 1> IPv6 전환기술에 따른 보안취약점

구분	취약점
터널링 (Tunneling)	- IDS, IPS 시스템 우회를 통한 네트워크 보안 위협 - 상대노드의 비인가된 터널링 생성으로 인한 보안상의 새로운 취약성 발생 가능
듀얼스택 (Dualstack)	- DHCP 등을 이용한 IP 주소 획득 - 비상태형 자동 주소설정 기법 등을 이용한 IP 주소 획득 - 예상치 못한 호스트간 터널링 발생으로 인한 의도하지 않은 새로운 취약성 발생 가능
IPv6 변환	- NAT-PT 장비 장애 및 서비스 중단으로 인한 공격자의 조작된 호스트 프리픽스 할당과 호스트로 전달될 모든 패킷 캐치 - 공격자가 스푸핑된 패킷을 IPv4로 다량 전송시에 주소풀에 등록된 IPv4 주소를 고갈시킴으로 인한 서비스거부공격의 발생 가능

IPv6가 도입되어 기존 IPv4 망과 새롭게 구성된 IPv6 망이 공존하게 되면, 보안 관점에서는 기존에는 없던 새로운 문제점들이 야기될 수 있다. 이러한 문제점들은 IPv4와 IPv6가 공존되는 기간 동안에 발생될 것이며, IPv6가 완전히 도입이 완료되고, IPv4가 사라지게 되면, 더 이상 이러한 문제는 없어질 것이다. 그러나 IPv4와 IPv6 전환 메커니즘들이 망 상에서 존재하고 동작하는 한, IPv4와 IPv6 연동 환경에서의 보안 문제점들이 계속 문제화될 것이다. 다음은 현재 IPv4 망에서 IPv6 망으로의 전환기술에서발생 가능한 보안 위협에 대한 세부 내용이다.

3.1 IPv4/IPv6 터널링 보안 취약점

일반적으로 터널링은 네트워크를 보호하기 위해 설치된 침입차단시스템이나 침입탐지시스템을 우회할 수 있기 때문에 네트워크상에서 발생하는 보안 위협이다. 인터넷망에서는 연결하고자 하는 상대 단말의 유형이나 서비스 등에 미리 확인할 수 없는 것이 일반적이다. 따라서 복잡한 터널링 구조를 갖는 IPv4와 IPv6 공존망에서는 상대에 대한 프로토콜 버전과 망 구조를 더욱 복잡하게 하여 상대노드에 대한 인증 등 미리 확인이 필요할 시에는 보안 관점의 문제들이 발생할 수 있다. 또한 IP-in-IP 패킷 상에서의 송신자 및 수신자 주소 등이 스푸핑(spoofing)되면, 또 다른 보안 문제를 야기시킬 수 있다.

3.2 IPv4/IPv6 듀얼스택 보안 취약점

IPv4/IPv6 듀얼스택 노드는 DHCP 등을 이용하여 해당 IPv4 주소를 얻고, 비상태형 자동 주소설정 기법 등을 이용하여 IPv6 주소를 획득할 수 있다. 따라서 듀얼스택 노드의 DNS는 도메인 네임과 IP 주소간 매핑을 위해 IPv4와 IPv6 모두를 지원해야 한다. 듀얼스택 호스트에 대한 중요한 보안 고려사항은 IPv4에서 요구되는 보안수준이 IPv6 상에서도 동일하게 적용되어야 한다. IPv4/IPv6 전환시 듀얼스택 클라이언트가 IPv4에 대해서만 IPsec-VPN을 지원하고 IPv6에 대해서는 지원하지 않는다면 IPv6 패킷에 대한 안전한 통신을 보장하지 못하게 된다.

3.3 IPv6 변환 기술의 보안 취약점

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 포트번호로 구분하는 기능을 갖는다.

IPv6 호스트 A가 IPv4 호스트 B로 패킷을 송신할 때, 그 패킷은 IPv6 주소를 가지므로 IPv4로 변환해야 한다. 이때 IPv6에서 생선된 체크섬 등은 사용할 수 없으며 NAT-PT를 사용하면 종단간 보안을 제공할 수 없다. 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 중단될 경우 공격자가 IPv6 호스트에 조작된 IPv6 프리픽스가 할당하여 IPv4 호스트로 전달될 모든 패킷을 가로챌 수 있다. NAT-PT 장비가 위치한 네트워크에서 공격자가 스푸핑 된 패킷을 IPv4 네트워크로 다량 전송하면 주소풀(Address pool)에 등록된 IPv4 주소를 고갈시켜 서비스거부공격이 가능해진다.

3.4 IPv6 전환기술의 보안 취약점 대응방안

현재까지 IPv4에서 IPv6의 자연스러운 이전을 지원해주는 IPv6 전환 매커니즘에 대한 많은 연구가 이루어졌다. 그러나 당분간 IPv4와 IPv6의 공존은 모두가 공감하고 있으며, 실제 IPv6 연동 환경에서 고려해야 할 전환 기술별 보안 취약점 대응방안은 다음과 같다.

듀얼스택에서는 IPv6의 새로운 기능을 인지함과 동시에 침입탐지, 모니터링, 로깅 및 감사기능을 업그레이드 하여 IPv4와 동일한 수준의 정보보호 대책이 필요하다. 터널링의 경우 터널링된 프래픽을 패킷필더, 안티바이러스, 방화벽, IDS 적책 등으로 검사하여 비인가된 터널링 트래픽을 차단 하는 등 터널링 트래픽을 IPsec으로 터널 종단간 암호화가 필요하다. 또한, IPv6 변환의 경우 NAT-PT에서 인그레스 필터링을 수행하고, 필터링을 통해 IPv4 소스 주소가 브로드캐스트 및 멀티캐스트 주소인 모든 패킷을 폐기함으로써 서비스거부공격에 대한 방지가 필요하다.

4. 결론

정보화 사회의 발달로 인한 인터넷 사용자 수의 증가는 인터넷 구조 자체를 새로운 방향으로 흐르게 하는 발판이 되었으며, 특히 인터넷 주소 고갈로 인한 기존의 IPv4에서 IPv6로 전환은 불가피한 상황이 되었다. 그러나 광대하게 퍼져있는 IPv4 인터넷을 한순간에 바꾸는 것은 거의 불가능 하며, 향후 몇 년간 IPv4 주소와 IPv6 주소가 공존할 것이기 때문에 IPv6로의 전환 기술 및 전환 환경에서의 위협요소와 보안 고려사항을 수용할 필요성이 있다.

이에 따라 본 논문에서는 기존의 인터넷 주소체계인 IPv4에서 차세대 인터넷 프로토콜인 IPv6로의 성공적인 전환체계를 확립하기 위하여 IPv4/IPv6의 전환 기술인 터널링, 듀얼스택, IPv6 변환 기술을 연구하였으며, 이에 동반한 IPv6 전환 환경에서의 보안 취약점 및 대응방안에 대하여 연구하였다. 향후 연구 방안으로는 IPv6 로의 안정적인 차세대 인터넷 사용망 전환을 위하여 전환 기술상의 보안 취약점 해결방안에 대하여 지속적인 연구가 필요하다.

ACKNOWLEDGMENT

본 연구는 경원대학교의 지원으로 수행되었음

참고문헌

[1] 이희철, 김형준, “IPv6 전환기술 동향 및 과제”, 한국인터넷정보학회, 2003

[2] E. Nordmark and R. E. Gilligan, “Basic Transaction Mechanisms for IPv6 Host and Routers”, IETF, draft-ietf-v6ops-mech-v2-02.txt, January 30, 2004.

[3] 한국인터넷진흥원, “http://www.kisa.or.kr/”

[4] 한국인터넷진흥원, “http://www.kisa.or.kr/”

[5] 티스토리닷컴, “http://www.koosal.tistory.com/”

[6] S.Satapati, “NAT-PT Applicability”, InternetDraft draft-satapati-v6ops-natpt-appli cability-00, Oct. 2003

[7] “Stateless IP/ICMP Transaction Algorithm (SIIT)”, RFC, 2765, Febuary, 2000.

[8] 정보흥, 임재덕, 김영호, 김기영, “IPv6 환경의 보안 위협 및 공격 분석”, 전자통신동향분석, 2007.