IPv4/IPv6 변환기술에서의 보안 취약점 분석 및 보안성 강화방안

정재홍*, 김진덕, 신용태
*숭실대학교 컴퓨터학과
e-mail:jhjung@cherry.ssu.ac.kr

IPv4/IPv6 Translation Technology and Enhanced Security Measures in the Analysis of Security Vulnerabilities

Jae-Hong Jung*, Jin-Duk Kim, YongTae Shin
*Dept of Computer Science, Soong-Sil University

요 약

기존 IPv4 주소의 고갈로 인해 IPv6로의 주소 전환이 예상되며, 이는 IPv4 네트워크와 IPv6 네트워크의 혼재 상황을 야기시킨다. 이는 IPv4 주소체계와 IPv6 주소체계가 다르므로 주소 전환 문제와 이에 따른 보안상의 문제가 발생 할 수 있다. 이를 해결하기 위해서 NAT-PT, NAT64와 같은 변환기술이 개발되었고, 각 네트워크에서의 보안기술도 개발되었다. 그러나 기존 연구는 각 네트워크에서의 보안 취약점 분석과 보안성 강화방안을 연구하였지만, IPv4/IPv6 혼재 상황에서의 보안 취약점에 관한 연구들은 부족한 실정이다. 본 논문에서는 향후 도래할 IPv4/IPv6 네트워크 혼재 상황에서 사용될 전환 기술 중 변환 기술인 NAT-PT와 NAT64를 중심으로 보안 취약점을 분석하고, 보안성 강화방안을 제시하였다.

1. 서론

최근 스마트폰, VoIP, IPTV 등 다양한 디바이스 보급 증가로 IPv4 주소는 고갈 되었고, IPv6로의 전환이 가속화 되고 있다. 이러한 IPv6로의 전환은 단시일에 이루어지는 것이 아니므로, IPv4와 IPv6의 공존을 위하여 많은 전환 기술들이 개발되었다.

IPv4는 보안을 고려하지 않고 설계되었기 때문에 보안에 취약한 특성을 가지며 IPv6로의 전환 환경은 IPv4의 취약점 및 IPv6의 취약점, 혼재상황에서의 취약점 등 보안적인 측면에서 기존 주소체계 보다 더욱 취약하다.

본 논문은 전환 기술 중 변환 기술을 중심으로, IPv4/IPv6 혼재 상황에서 발생 할 수 있는 보안 취약점을 분석하고 보안성 강화방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 변환 기술인 NAT-PT[1]와 NAT64[2] 동작방식 및 특징을 기술하며, 3장에서 NAT-PT와 NAT64 기술의 보안 취약점 및 보안성 강화방안을 제시한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련연구

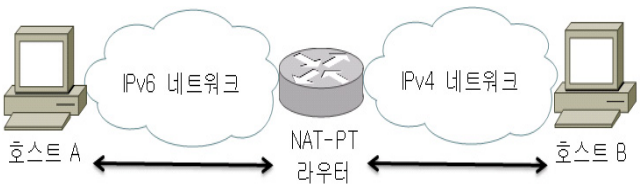
전환 기술은 IPv4 네트워크에서 IPv6 네트워크로 넘어가기 위해 필수적으로 요구되는 기술로 크게 듀얼스택, 터널링, 변환 기술로 분류된다. 이 중 변환기술은 IPv4네트워크와 IPv6네트워크 서로 상호통신을 하기 위해 사용된다.

IPv4와 IPv6는 헤더 구조 및 길이가 다르기 때문에 이 둘이 서로 통신을 할 때에는 각자에게 맞는 IP 형태로 변환하는 과정이 필요하다. 이러한 변환 기술로 NAT-PT, NAT64가 있다.

2.1 NAT-PT(Network Address Translation/Protocol Translation)

NAT-PT는 IPv4 주소 풀에서 동적으로 IPv4 주소를 할당해 주는 NAT(Network Address Translation)[3] 기능과 SIIT(Stateless IP/ICMP Translator)[4] 기능, 그리고 어플리케이션에 따라 발생하는 추가적인 요구사항을 변환해주는 ALG(Application Level Gateway) 기능으로 이루어져 있다. NAT-PT의 IPv6 주소는 /96 크기의 IPv6 프리픽스와 IPv4 주소로 구성된다[5].

NAT-PT는 각 네트워크상의 노드들이 듀얼스택을 탑재하지 않고 통신 할 수 있다는 장점이 있다. 그러나 NAT-PT는 IP계층의 주소변환만 수행하므로, 어플리케이션에서 IP를 사용하는 경우 어플리케이션을 지원하는 ALG가 필요하다[6].



(그림 1) NAT-PT의 구성

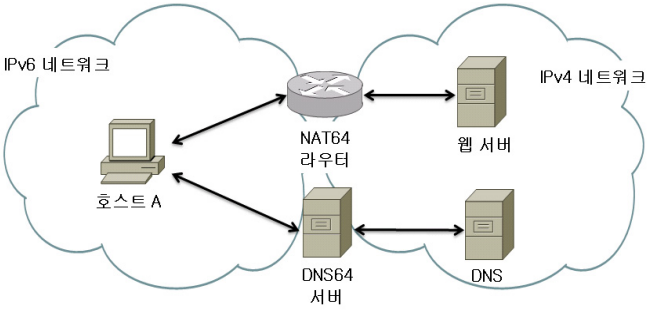
(그림 1)은 IPv6 네트워크 내부의 호스트 A와 IPv4 네트워크의 호스트 B가 상호통신을 하기 위해 NAT-PT를 사용하는 동작과정을 보여준다.

호스트 A는 NAT-PT에게 IPv6 패킷을 전송한다. NAT-PT 라우터는 IPv6 패킷의 목적지 주소를 확인하여, 매핑 정보에 맞게 출발지와 목적지 주소를 IPv4 주소로 변환 후, 호스트 B에게 IPv4 패킷을 전송한다[7].

2.2 NAT64

NAT64는 DNS64와 더불어 IPv6 네트워크의 클라이언트가 IPv4 네트워크의 서버로 통신을 할 수 있도록 하는 변환 메커니즘이다. NAT64는 기본적으로 IPv6 클라이언트가 IPv4 서버로 통신을 하는 것을 지원하나, NAT64가 IPv6 네트워크의 클라이언트에 대한 정적으로 구성된 바인딩 정보를 가지고 있을 경우, IPv4에서 IPv6로의 통신도 가능하다.

NAT64와 DNS64는 적용이 쉽고 기존의 IPv6와 IPv4 장비에 변화를 주지 않고 적용할 수 있다는 장점이 있다.



(그림 2) NAT64의 구성

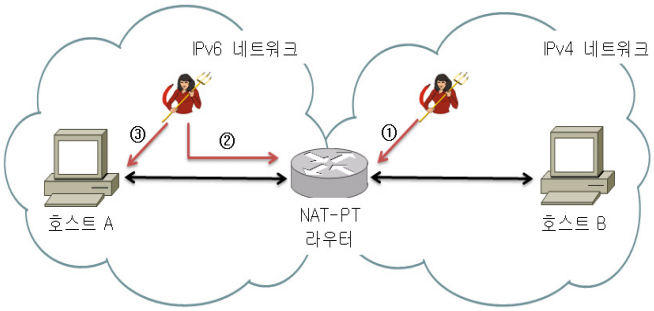
(그림 2)는 IPv6 네트워크의 호스트 A가 IPv4 네트워크의 웹서버와 통신 하고자 할 때의 동작과정을 설명한다.

호스트 A는 DNS64로 웹 서버의 도메인 이름에 대한 IP 주소를 요청한다. DNS64는 DNS와 통신하여 웹서버의 IPv4 주소를 얻게 되고, NAT64의 IPv6 프리픽스를 붙여 호스트 A로 전송한다. 그리고 호스트 A는 NAT64 라우터로 TCP SYN 패킷을 전송한다. NAT64는 사용하지 않은 포트를 IPv4 주소와 매핑하여 NAT64의 매핑 테이블을 구성한다. 이후, NAT64는 IP/ICMP 변환 알고리즘을 사용하여 IPv6 헤더를 IPv4 헤더로 변환하여 웹 서버로 전송한다[2].

3. 변환 기술의 보안 취약점 및 보안성 강화 방안

3.1 NAT-PT의 보안 취약점 및 보안성 강화 방안

NAT-PT에서 발생할 수 있는 보안 취약점은 서비스 거부공격, MITM공격, 스니핑, 스푸핑이 있다. 이를 자세히 살펴보면 다음과 같다.



(그림 3) NAT-PT의 보안 취약점

◎보안 취약점

① (그림 3)에서와 같이 IPv6 네트워크에 있는 호스트 A가 IPv4 네트워크에 있는 호스트 B로 패킷을 보낼 때, 공격자는 NAT-PT 라우터에게 전송하는 패킷을 가로채 최소 크기로 조각내서 NAT-PT 라우터로 전송한다 이때, NAT-PT 라우터는 패킷을 재조합하는 과정에서 버퍼 과부화와 CPU의 자원이 크게 소모되어 서비스거부공격이 발생한다.

② (그림 3)에서 공격자는 IPv6 네트워크의 호스트 A에 대한 IPv6 주소를 스푸핑하여 공격자가 IPv6의 소스주소를 다량으로 생성하고 NAT-PT 라우터로 전송함으로써 NAT-PT 라우터가 가진 IPv4 주소 풀을 모두 고갈시킬 수 있다.

③ (그림 3)에서와 같이 IPv6 네트워크에 있는 공격자가 NAT-PT 라우터처럼 가장하여 IPv6 호스트 A에 조작된 IPv6 프리픽스를 할당하여, 패킷을 가로챌 수 있다.

이러한 NAT-PT에서 발생할 수 있는 보안 취약점에 대응하기 위한 보안성 강화 방안은 다음과 같다.

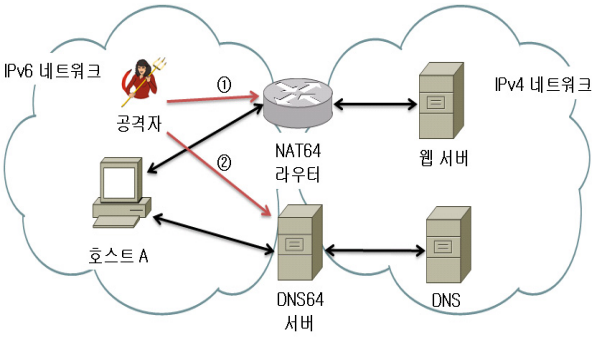
◎보안성 강화방안

① NAT-PT 라우터는 최소 크기로 조각난 첫 번째 패킷을 받으면 그 패킷의 필요한 모든 헤더 정보를 충분히 가질 수 있는 크기인지를 검증해야 하며 NAT-PT 라우터에서 패킷필터링의 기능을 수행해야 한다.

② IPv6 호스트 A의 TCP/UDP 포트를 IPv4 호스트 B의 주소에 부합하는 TCP/UDP 포트로 매핑을 지원하는 NAT-PT에 인증기술(포트인증) 사용을 통해 IPv4 주소 풀 고갈을 방지해야 한다.

③ 위조된 IPv4(혹은 IPv6) 패킷과 정상적인 IPv4(혹은 IPv6) 패킷을 구분할 수 있는 방안과 공격자가 출발지 주소를 위조하지 못하게 하는 SEND[8] 기술의 보안 옵션 CGA을 설정하여 공격자로부터 패킷을 보호 할 수 있다.

3.2 NAT64의 보안 취약점 및 대응방안



(그림 4) NAT64의 보안 취약점

NAT64에서 발생할 수 있는 보안 취약점은 서비스거부공격, MITM 공격, 캐쉬 포이즌 공격이 있다. 이를 자세히 살펴보면 다음과 같다.

◎보안 취약점

① (그림 4)와 같이 IPv6 네트워크의 호스트 A가 IPv4 네트워크의 웹 서버와 서로 통신을 하려고 할 때, 공격자는 출발지 IPv6 주소를 변경하여 다량의 패킷을 NAT64 라우터로 전송하면 NAT64의 자원(프로세스, 메모리)을 고갈시킬 수 있다.

② (그림 4)와 같이 공격자가 DNS64 서버에게 IPv4의 바인딩 주소를 추측할 수 있다면 대량의 패킷을 바인딩한 IPv4 주소로 전송하여 NAT64 내부에서의 Hairpinning 루프를 발생할 수 있다. 그리고 DNS 서비스는 UDP기반 네트워크 서비스를 제공하므로 패킷 검증에 대한 매커니즘을 가지고 있지 않다. 따라서 공격자가 DNS64에 위,변조된 패킷을 삽입함으로 인해 DNS서비스의 기능을 마비시키거나 캐쉬 포이즌 공격을 할 수 있다.

이러한 NAT64에서 발생할 수 있는 보안 취약점에 대응하기 위한 보안성 강화 방안은 다음과 같다.

◎보안성 강화방안

① NAT64 라우터는 IPv6 주소를 검증하여 보호할 수 있다. 즉, SYN 패킷의 IPv6 주소가 실제 사용되는 정상적인 IPv6 주소인지를 검증해야 하며. SEND의 CGA를 사용하여 공격자로부터 자원을 보호 할 수 있다.

② NAT64 라우터는 바인딩 테이블을 검사하여 출발지 주소에 프리픽스64를 포함하여 수신되는 패킷을 필터링하여야 한다. 그리고 송신자가 전송한 메시지를 DNS64가 발신인증으로 검사하고, DNS서버에서 전송되는 데이터에 대한 위,변조에 무결성을 제공할 수 있어야한다.

4. 결론

본 논문에서 NAT-PT와 NAT64는 스니핑, 스푸핑을 기반으로 서비스거부공격, MITM, 캐쉬 포이즌 공격에 대해 보안이 취약한 것으로 분석하였다. 이에 대한 강화방안으로는 본 논문에서 SEND의 CGA, 패킷필터링, 데이터발신인증, 포트인증 등과 같은 다양한 인증기술을 제시하였다.

향후 연구에서는 본 논문에서 제시한 것과 더불어 전환 기술 전체에 대한 보안 취약성을 분석하고 보안성 강화 방안의 지속적인 연구가 필요하다.

참고문헌

[1] G. Tsirtsis, P. Srisuresh, “Network Address Translation Protocol Transation (NAT-PT),” RFC2766, 2000.2.

[2] M. Bagnulo, P. Matthews, “Stateful NAT64: Network Address and Protocol Translation from IPv6 clients to IPv4 Servers,” RFC6146, 2011.4.

[3] Egevang, K. and R. Atkinson, “IP Encapsulating Security Payload (ESP),” RFC2406, November 1998.

[4] Nordmark, E., “Stateless IP/ICMP Translator(SIIT).” RFC2765, 2000. 2.

[5] 현정식, 황윤철, 정윤수, 이상호, “NAT-PT를 고려한 단대단 IPSec 보안 매커니즘,” 정보과학회 논문지, vol.30 no.5, pp.604-613, 2003.10.

[6] 최인석, 정수환, 김영한, 박용석, “IPv6 전환 기술 중 NAT-PT에서의 IPSec 적용 방안,” 한국통신학회 논문지, 30(11B), pp.736-743, 2005.11.

[7] 전현호, “IPv6 라우팅 Routing,” NEVER STOP, pp.529-568, 2009.9.

[8] 박소희, 나재훈, 정교일, “IPv6의 SEND 표준화 동향,” ITFIND, 2004.