IPv6 및 IPv4/IPv6 전환기법에 대한 보안 취약점 조사

김주호*, 이재훈**, 박능수*
*건국대학교 컴퓨터정보통신공학과
**동국대학교 정보통신공학과
e-mail : juho0719@naver.com

IPv6 and IPv4/IPv6 Translation Security Vulnerability

*Juho Kim, **Jaehwoon Lee, *Neungsoo Park
*Dept. of Computer Science and Engineering, Konkuk University
**Dept. of Information and Communication Engineering, Dongguk University

요 약

현재 IPv4 주소가 고갈됨으로써 IPv6 를 사용할 수 밖에 없는 상황에 놓여지게 되었다. 그리고 IPv6 주소체계를 이용하다 보니 이에 따른 보안취약점들이 발견되었다. IPv6 보안취약점에는 확장헤더, ICMPv6, NDP, 다양한주소에 따른 취약점들이 있다. 이것뿐만 아니라 IPv4 와 IPv6 네트워크 간에 통신이 가능한 6to4, ISATAP, Tunnel Broker, Teredo 와 같은 기술이 나오게 되었고, 이러한 것들 또한 보안취약점이 발견되었다. 6to4 보안취약점에는 분산반사 스푸핑 트래픽 공격이 있고, Teredo 에는 로컬 peer 발견 절차에 다른 캐쉬 오버플로우 공격이 있다. 그리고 ISATAP 에는 라우터를 가장한 MITM 공격이 있고, Tunnel Broker 에는 Tunnel Borker 와 Tunnel Server 를 위장하여 공격하는 방법이 있다. 이렇게 IPv6 주소체계로 바뀌면서 생기는 새로운 보안취약점들에 대응하기 위해 현재 존재하는 라우터 같은 네트워크장비들도 보안취약점에 대응할 수 있는 변화가 필요하다

1. 서론

최근 ICANN 에서는 “IPv4 주소가 완전히 고갈되었다.”라고 발표함에 따라 앞으로는 IPv6 를 사용할 수 밖에 없는 상황에 놓여지게 되었다. 그리고 IPv6 주소체계를 이용하다 보니 이에 따른 보안취약점들이 발견되었다. 이것뿐만 아니라 IPv4 와 IPv6 네트워크간에 통신이 가능한 6to4, ISATAP, Tunnel Broker, Teredo 와 같은 기술이 나오게 되었다. 이에 따라 네트워크 장비들도 변화가 필요하게 되었고, 이미 나와있거나 앞으로 나올 IPv6 네트워크장비들도 보안취약점에 대응하기 위해 어떤 보안취약점들이 있는지 조사하였다

2. IPv6 보안취약점

2.1 확장헤더

IPv6 는 IPv4 헤더의 필드를 수정/삭제하거나, 확장헤더로 넘겨 전체크기를 개선하였다. 이로 인해 오버헤드를 줄이고 처리 효율을 높였지만, 그로인해 새로운 보안취약점들이 생겨났다.[1]

2.1.1 라우팅헤더의 보안 취약점

· 방화벽 우회 공격

그림 2-1 에서 공격자 A 는 서버 B 로는 접근이 가능하지만 서버 C 로는 접근할 수 없도록 설정되어 있다고 가정한다. 서버 B 라우팅 헤더의 Segment Left 필드 값이 1 이상인 경우에 공격자는 서버 B 를 경유하여 서버 C 로 공격 트래픽을 전달할 수 있다. 이런 점을 이용하여 공격자 A 는 라우팅 헤더를 이용 서버 C 로 패킷을 전달할 수 있어 방화벽의 정책을 우회할 수 있다.

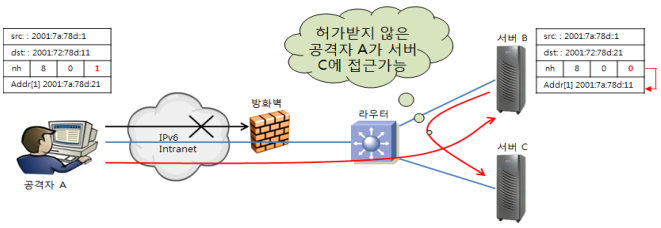

그림 2-1 방화벽 우회 공격

· 우회 공격

그림 2-2 는 라우팅 헤더를 이용 추적 우회 가능성을 나타낸다. 공격자는 공격 패킷의 주소를 희생호스트 주소로 위장하고, 라우팅 헤더를 이용하여 해당 패킷이 목적지인 Reflector 에 도달하기 전에 여러 라우터들을 거치도록 함으로써 추적을 어렵게 만들 수 있다

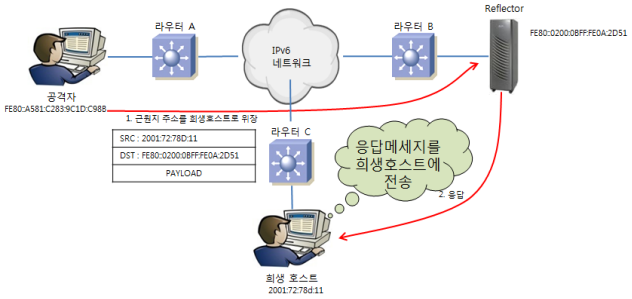

그림 2-2 라우팅 헤더를 이용하여 추적 우회

2.1.2 단편화 헤더의 보안 취약점

· 단편화 패킷 중복 공격

그림 2-3 과 같이 공격자가 패킷을 단편화하여 중복되게 패킷을 보냈을때 방화벽이 중복된 단편화 패킷을 필터링하지 못한다면, 임의의 호스트는 분할된 패킷을 재조립할 때 중복된 단편화 패킷 중 어떤 패킷이 올바른 것인이 판단할 수 없게 된다.

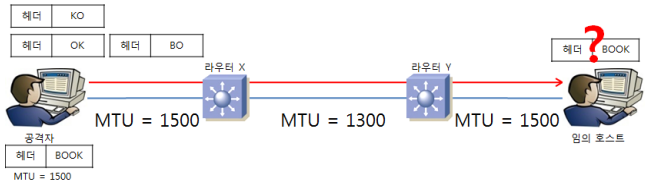

그림 2-3 단편화 패킷 중복 공격

2.2 ICMPv6

ICMPv6 에서는 중계 라우터에서 수신한 패킷의 크기가 다음 전달할 MTU 보다 큰 경우에는 packet too big 이라는 응답 메시지를 전송하게 된다. 이를 악용하여 그림 2-4 와 같이 공격자는 자신의 주소를 희생호스트 주소로 바꾸고, 라우터 X 로 1400 크기의 패킷을 전달하면 라우터 X 는 이를 받고 다음으로 전달 하려고 할 때 MTU 크기가 작아 패킷을 전달 할 수 없게 되어 packet too big 이라는 메시지를 반환하게 된다. 하지만 앞에서 공격자가 자신의 주소를 희생호스트로 바꾸었기 때문에 응답메시지가 희생호스트로 가게 됨으로써 서비스거부공격을 할 수 있게 된다.[1]

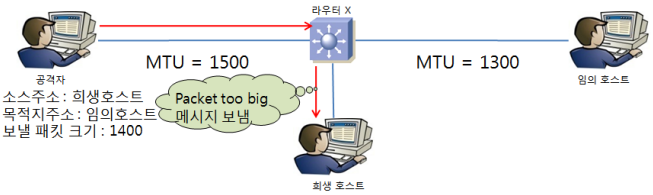

그림 2-4 ICMPv6 에러메시지를 이용한 DoS 공격

2.3 NDP

NDP 는 호스트가 연결된 링크상의 라우터 탐색, 프리픽스 정보 탐색, 파라미터 정보의 탐색, 호스트 주소 자동 설정 등의 역할을 한다. 이에 대한 보안취약점들은 다음과 같다.[2][3]

공격	설명
NS/NA 위장공격	- NS/NA 메시지를 위장, 희생자 호스트에 잘못된 네이버 캐시 엔트리를 생성. - 잘못 생성된 네이버 캐시 엔트리에 지정된 링크 계층 주소를 가진 노드를 경유하여 패킷을 전달(경로 우회)
NUD 실패유도	- 공격자가 희생호스트에 잘못된 네이버 캐시 엔트리를 생성하여 NUD 메커니즘 수행을 유발 - 노드가 네이버 캐시 엔트리를 삭제하면 반복적으로 위장된 NA메시지를 보냄으로써 NUD 실패를 유도

표 2-1 라우터/라우팅 메커니즘과 관련 없는 공격

공격	설명
라우터 위장공격	- 공격자가 RA 메시지를 보내어 자신을 디폴트 라우터로 알게 함. - 패킷전달경로 우회와 DoS 공격가능
redirect 위장 공격	- 리다이렉트 메시지를 위장하여 모든 패킷이 공격자를 지나가도록 설정하여 경로 우회 공격, DoS공격 가능
On-Link 프리픽스 위장공격	- RA 메시지의 프리픽스 주소 옵션을 위장 - 다른 네트워크에 속한 호스트들까지 링크상에 존재하고 있다고 착각하게 하여 서비스 거부 공격 가능
디폴트라우터 삭제	- 합법적인 라우터에 DoS 공격을 하여 RA 메시지를 전송할 수 없게 만듦 - 다른 네트워크로의 통신을 방해

표 2-2 라우터/라우팅 메커니즘과 관련 공격

2.4 IPv6 의 다양한 주소

IPv6 주소는 크게 유니캐스트, 애니캐스트, 멀티캐스트 주소 형태로 나뉜다.

2.4.1 사이트 범위를 갖는 멀티캐스트 주소

IPv6 에서는 브로드캐스트 주소 대신에 멀티캐스트 주소를 이용하여 브로트캐스트 서비스를 제공한다. 표 2-3 과 같이 공격자는 모든 라우터를 나타내는 주소와 모든 DHCP 서버를 나타내는 주소를 목적지 주소로 사용하여 범람 공격을 할 수 있다.

멀티캐스트 주소	의미
FF05::2	모든 라우터를 지칭
FF05::3	모든 DHCP 서버를 지칭

표 2-3 멀티캐스트 주소

2.4.2 애니캐스트 주소

애니캐스트 서비스에서 인증절차를 거치지 않으면, 인증되지 않은 애니캐스트 그룹 멤버가 거짓정보를 광고할 수도 있고, 송신자의 주소를 변경할 수 있기 때문에 이를 이용한 위장공격 및 서비스거부공격이 가능하다.

3. IPv4/IPv6 전환기술의 보안취약점

3.1 6to4 보안 취약점

3.1.1 분산 반사 스푸핑 트래픽 공격

스푸핑 IP 를 이용한 반사(Reflecting)트래픽 위협은 6to4 공격자가 자신의 주소를 VICTIM 노드의 주소로 바꾸어 Reflector 에 패킷을 보내면 중간 Reflector 는 응답을 바뀐 VICTIM 주소로 보내게 되어 공격을 당할 수 있다. [4][5]

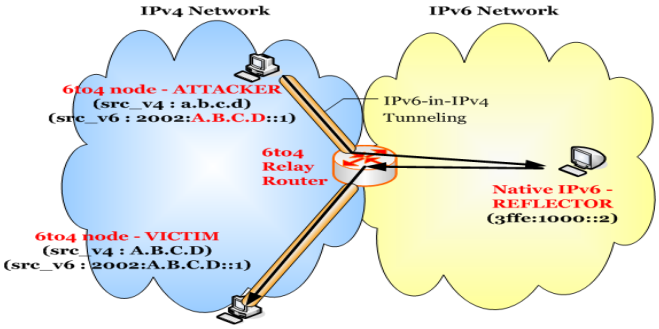

그림 3-1 분산 반사 스푸핑 IP 공격 시나리오

3.2 Teredo 보안 취약점

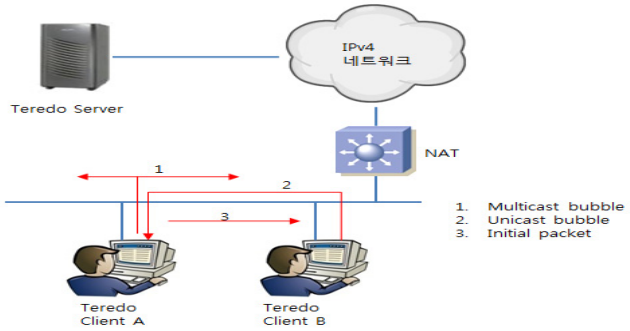

그림 3-2 로킬 peer 발견 절차

Teredo Client A 가 공격자인 경우 로컬 링크에 존재하는 Teredo Client 에 대한 Unicast 주소를 알 수 있고, 이를 이용하여 DoS/MITM 공격을 할 수 있다. Teredo Client B 가 공격자인 경우 Teredo Client A 가 Teredo 발견 요청 메시지를 보냈을 때 Teredo client B 는 스푸핑된 Teredo Unicast 응답 메시지를 보내고 Teredo Client A 는 B 가 보낸 불법적인 노드의 정보를 저장하게 된다. 이 후 Client B 가 응답 패킷을 위조해서 Teredo Client A 로 보내고, Client A 는 이 정보를 캐쉬에 저장하게 된다. 캐쉬의 저장공간은 한정되있기 때문에 Client B 가 다량의 패킷을 보내는 경우 오버플로우를 발생시킬 수 있다. [6][7]

3.3 ISATAP 보안 취약점

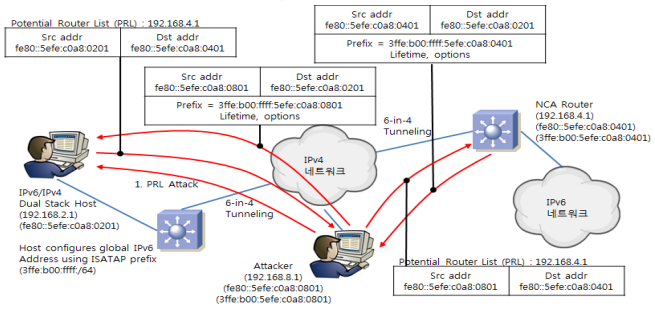

그림 3-3 라우터를 가장한 공격자에 의한 MITM 공격

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

호스트는 주소를 구성하기 위해 ISATAP 프리픽스를 요청하게 되면 등록된 PRL 리스트에서 라우터를 선택하여 그쪽으로 요청 패킷을 보내게 된다. 이 때 공격자가 PRL 리스트에 미리 자신의 주소를 등록시켜놓고, 자신을 선택하게 하면, 요청 패킷은 공격자에게 전송되고 공격자는 패킷을 변경하여 정상적인 라우터로 전송하게 된다. 다시 정상 라우터로부터 수신된 응답 패킷을 공격자가 수정하여 호스트로 보내면, 이 후의 모든 패킷은 공격자를 거쳐 송수신된다.

3.4 터널브로커 보안 취약점

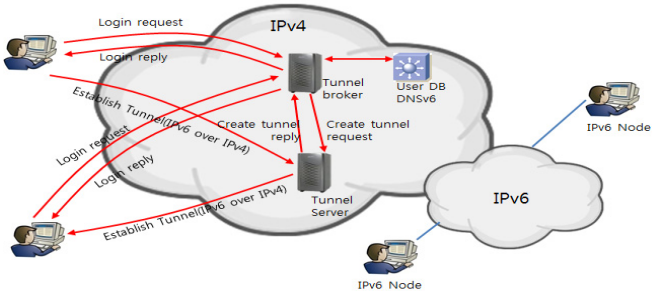

그림 3-4 터널 브로커에 의한 공격

듀얼스택 노드는 터널브로커로 로그인 요청을 보내면 터널브로커는 듀얼스택 클라이언트로부터 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.

4. 결론

이와 같이 새로운 주소체계인 IPv6 를 사용하거나, IPv4 에서 IPv6 로 변환할 때 생기는 보안취약점들이 많았다. 이에 따라 네트워크장비(라우터등)나 방화벽의 개선을 통해 위의 보안취약점들이 개선해야 되고, 그래야 앞으로 새로운 주소체계를 사용했을 때 보안위협을 피할 수 있다.

참고문헌

[1] 이영수, 박남열, 김용민, 노봉남, “IPv6 순수망과 IPv4/IPv6 혼재망의 보안취약점”, 한국정보보호학회 하계정보보호학술대회 논문집 Vol. 16 No.1, June 2006

[2] 신명기, “IPv4/IPv6 연동환경에서의 차세대 보안 기술”, 전자공학회지 제 33 권 제 8 호, Aug. 2006

[3] P. Nikander, J.Kempf, E. Nordmark, “IPv6 Neighbor Discovery trust models and threats”, InternetDraft, draft-ietf-send-psreg-03.txt, Apr. 2003

[4] Alefiya Hussain, John Heidemann, Christos Papadopoulos, “A Framework for Classifying Denial of Service Attacks. Technical Report”, ISI-TR-2003-569, USC/Information Sciences Institute, Feb. 2003

[5] P. Ferguson and D. Senie “Network Ingress Filtering:

Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2267, Jan. 1998
[6] J. Hoagland and S. Krishnan, "Teredo Security Concerns", Internet Draft, draft-ietf-v6ops-teredo-security-concerns-02.txt, Feb. 2008
[7] 김미영, 문영성, "IPv4/IPv6 변환기 보안 위협", 한국통신학회지 제 23 권 제 9 호, Sep. 2006
[8] A. Conta, S. Deering and M. Gupta, "Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, Mar. 2006
[9] T. Narten, E. Nordmark, W. Simpson and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, Sep. 2007.
[10] 김정욱, "IPv6 보안 취약점에 대한 분석 및 시나리오 기반 실험", 석사학위논문, 전남대학교, Feb. 2008.
[11] 신동명, 현호재, 윤미연, 원유재, "IPv6 보안 위협 및 대응 방안", 정보처리학회지 제 16 권 제 3 호, Feb. 2006.
[12] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture", RFC 3513, Feb. 2006.
[13] F. Templin, T. Gleeson, and D. thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, Mar. 2008.
[14] A. Durand, P. Fasano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker", RFC 3053, Jan. 2001
[15] Alefiya Hussain, John Heigemann, and Christos Papadopoulos, "A Framework for Classifying Denial of Service Attacks. Technical Report", ISI-TR-2003-569, USC/Information Sciences Institute, Feb. 2003.
[16] 허석열, 이완직, 신범주, 한기준, "안전한 Teredo 서비스를 위한 패킷 필터링 메커니즘 설계 및 구현", 한국산업정보학회논문지 제 12 권 제 3 호, Sep. 2007.