IPv6 순수망과 IPv4/IPv6 혼재망의 보안 취약점

이영수*, 박남열**, 김용민***, 노봉남****

*전남대학교 정보보호협동과정

**전남대학교 시스템보안연구센터

***전남대학교 전자상거래전공

****전남대학교 전자컴퓨터정보학부

A Security Vulnerability in IPv6 Native Network and Mixed IPv4/IPv6 Network

Young-Soo Yi*, Nam-Youl Park**, Yong-Min Kim***, Bong-Nam Noh****

*Interdisciplinary Program of Information Security, Chonnam National University

**System Security Research Center, Chonnam National University

***Dept. of Electronic Commerce, Chonnam National University

****Div. of Electronics, Computer and Information Eng., Chonnam National University

요 약

IPv6는 차세대 네트워크를 구축하기 위한 가장 핵심적인 기술로써, 풍부한 주소공간과 이동성 지원, 보안기능 강화 등 IPv4에 비해 많은 이점을 지니고 있다. 또한 IPv4의 주소 고갈 문제를 해결하기 위해 IPv6로의 전환이 당연시 되고 있으나 IPv4/IPv6 혼재망이 과도기적인 입장에서 대안이 될 수 있다. 그러나 IPv4/IPv6 혼재망과 IPv6망은 IPv4에서와 마찬가지로 프로토콜 기능상의 많은 문제점을 안고 있다. 본 논문에서는 IPv6망 및 IPv4/IPv6 혼재 네트워크상에서의 보안 취약점과 실험 결과를 기술하였다.

Ⅰ. 서론

현재의 IPv4의 주소체계는 인터넷 사용자의 급속한 증가로 인해 주소고갈 문제에 직면하고 있다. 이러한 문제를 해결하기 위한 임시적인 해결책으로 CIDR, NAT, DHCP 등을 이용하여 사용하고 있으나, 궁극적으로 주소 고갈을 막는 해결책은 되지 않는다. 이를 위하여 인터넷 주소 제공 및 관리를 위한 장기적이고 근본적인 해결책인 IPv6로의 전환이 필요 하다고 할 수 있다. 그러나 현재 IPv6는 IPv4와 마찬가지로 많은 보안상의 취약점을 안고 있다. 이러한 취약점에 대한 정확한 보안 프레임워크가 정의되어 있지 않은 상황에서 IPv6로의 전환은 많은 문제점을 일으킬 수 있다.

본 논문에서는 IPv4/IPv6 혼재망 및 IPv6에서의 보안상 문제점에 대해 기술을 하고 ICMPv6를 이용한 보안 취약점중에 하나인 "Packet too Big" 메시지를 이용한 DoS 공격 실험 결과를 기술하였다.

Ⅱ. 관련연구

IPv6[1]의 특징으로는 "풍부한 주소 공간", "헤더 처리의 효율성", "보안성 제공", "이동성 제공" 및 "주소 관리의 효율성 제공" 측면으로 분류할 수 있다.

IPv6는 128비트의 주소 체계를 가지고 있다. 3.4 × 1038 만큼의 주소 공간을 생성할 수 있으며 이는 거의 무한대에 이르는 숫자로 주소 고갈 문제는 더 이상 제기되지 않을 것으로 보인다.

또한 IPv6는 복잡한 헤더 형식을 단순화 시켰다. 주소 공간의 증가로 인하여 헤더의 크기는 증가를 하였지만 헤더 규격이 단순화되었으며 사용하지 않는 필드를 삭제하거나 확장 헤더로 넘겨 오버헤더를

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

줄임으로 처리 효율을 높였다.

이동성이 고려되지 않은 IPv4에 비해 IPv6는 Routing 헤더와 바인딩 업데이트 기능을 이용, 라우팅 최적화를 통해 IPv4의 삼각 라우팅 문제를 없애주고 주소 자동 설정에 의해 임시 주소를 쉽게 구현하였다. 또한 주소 자동 설정에 의해 임시 주소를 쉽게 구현 할 수 있다. 이러한 동작은 앞으로 모바일 환경에서의 네트워크 지원을 더욱 수월하게 해 줄 수 있다.

IPv6는 주소 공간이 늘어난 만큼 IP 주소를 할당하고 관리하는 것이 쉽지 않다. 이러한 대안으로 "자동 주소 구성" 기능을 제공 함으로 IPv4에 비해 주소 공간 관리의 효율성을 증대 시켰다.

IPv4는 연결된 호스트 간에 데이터 교환에만 중점을 두었기 때문에 보안상 고려가 이루어 지지 않았다. 이에 반해 IPv6는 기본적으로 확장 헤더를 통해 IPSec을 기본적으로 지원하여 기밀성 및 무결성, 데이터 근원 인증 및 재연공격 방지 서비스 등을 제공 할 수 있게 되었다.

Ⅲ. 차세대 네트워크 보안 위협 사항

3.1 IPv6 프로토콜 보안 위협 사항

이번 절에서는 순수 IPv6 네트워크에서 일어날 수 있는 프로토콜의 보안 위협[2]들에 대해 기술한다. 패킷 스니핑, 패킷 스푸핑, 중간자 공격, 그리고 IP 상위 계층의 취약점 공격과 같은 IPv4의 보안 취약이 그대로 적용이 가능하며 확장 헤더와 새로운 기능 추가로 인한 새로운 취약점도 발견이 되었다[2].

3.1.1 라우팅 헤더 보안 취약성

IPv6에서는 확장 헤더인 라우팅 헤더를 이용하여 방화벽을 우회할 수 있다. 네트워크의 특정 호스트로 가는 트래픽을 막는 방화벽을 우회하기 위하여 소스 라우팅 기법을 이용, 동일네트워크의 다른 호스트를 경유하는 방법이 존재한다.

3.1.2 Site-Local scope 멀티캐스트 주소 취약성

IPv6는 모든 라우터를 나타내는 주소 FF05::2와 모든 DHCP를 나타내는 주소 FF05:3 을 제공하고 있다. 위 주소를 목적지 주소로하여 사이트에 존재하는 모든 라우터 또는 DHCP에 대한 주소 스캔 작업 없이 플러딩 공격을 시행 할 수 있다. 또는 응답을 이용하여 모든 라우터 또는 DHCP에 대한 정보를 얻어 올 수도 있다.

3.1.3 ICMPv6 보안 취약성

IPv6 라우터는 수신한 패킷의 크기가 다음 링크의 MTU보다 큰 경우 "Packet too Big"이라는 ICMPv6 메시지를 송신자에게 전송하여 경로상의 오류를 알려준다. 악의적인 공격자는 MTU보다 큰 패킷을 연속적으로 전송하여 특정 호스트에 "Packet too Big" 메시지를 이용한 DoS 공격을 시도할 수 있다.

Hop-by-Hop 확장 헤더 또는 Destination Options 확장헤더에 옵션 값이 잘못 설정 된 패킷을 수신할 경우에는 "Parameter Problem" 응답 메시지를 송신자에게 전송한다. 이 메시지를 이용하여 "Packet too Big"을 이용한 공격과 같은 공격을 할 수 있다.

IPv6 자동 주소 구성 기능을 제공하기 위하여 라우터는 RA(Router Advertisement) 메시지를 주기적으로 네트워크에 전송한다. 공격자는 이 메시지를 이용하여 링크 MTU, 가능 도달 시간, 재발송 시간, Prefix등의 정보를 수집할 수 있다.

3.1.4 애니캐스트 보안 취약성

애니캐스트 요청에 대해 유니캐스트 주소로 응답을 함으로 공격자는 망 내부의 topology가 유추된다. 공격자는 이 정보를 이용하여 공격 대상을 선정 할 수 있다.

3.1.5 패킷 단편화 보안 취약성

악의적인 공격자는 단편화 패킷의 offset 값을 조작하여 패킷 헤더의 특정 내용을 변경 할 수 있다. 이 취약점은 두 번째 패킷이 첫 번째 패킷의 포트 번호를 덮어 씀으로써 방화벽을 우회하는데 쓰일 수 있다.

첫 번째 단편화 패킷을 조그마하게 하여 방화벽이 체크하는 헤더 부분의 일부분을 다음 패킷에 넣도록 하는 방법으로 방화벽을 우회할 수 있다.

악의적인 공격자는 단편화 패킷의 마지막 패킷을 전송하지 않음으로 공격 대상이 된 호스트의 버퍼 사용량을 증가 시켜 시스템 오작동을 유발 할 수 있다.

3.1.6 IPv6 확장 헤더의 보안 취약성

알려지지 않은 확장 헤더나 목적지 옵션을 갖는 패킷의 사용으로 시스템의 오작동을 유발 할 있다.

Hop-by-Hop 옵션 헤더를 남용 하면 중계 라우터가 처리해야하는 정보가 늘어나게 된다. 이러한 패킷을 대량 발생시키면 패킷의 경로에 있는 모든 중계 라우터의 동작을 지연시킬 수 있다.

Router Alert Option은 중계 라우터가 패킷을 정밀하게 검사하도록 요구한다. 이 옵션을 남용하게 되면 패킷의 경로에 있는 모든 라우터의 동작을 지연 시킬 수 있다.

3.2 IPv4/IPv6 혼재망의 보안 위협

3.2.1 신뢰성 없는 라우터

DSTM, ISATAP[3], Teredo[4] 등 현재 지원되고 있는 터널링 기법들은 클라이언트가 터널링 라우터들에 대한 인증을 수행하지 않는다. 이러한 경우 라우터로 가장한 악의적인 공격자는 클라이언트에게 잘못된 네트워크 구성 정보를 전송하거나 악의적인 호스트 정보를 전송하여 원활한 통신을 방해 할 수 있다.

3.2.2 신뢰성 없는 DNS 또는 DHCP

터널링 기법들 중에서 내부 네트워크 IP를 구성하기 위하여 DHCP를 사용하는 경우가 있다. 그러나 이 DHCP에 대한 인증이 없을 경우, 악의적인 공격자는 DHCP 혹은 DNS로 위장하여 잘못된 주소 구성을 유도 원활한 통신을 방해 할 수 있다.

3.2.3 오버플로우

DSTM 서버는 DHCPv6[5]를 이용하여 터널링에 이용할 주소공간을 관리하고 있다. 클라이언트에 대한 사용 인증을 하지 않는 DSTM 서버는 악의적인 공격자의 다량의 DHCP 요청에 의해 과부하가 초래될 수 있으며, 관리중인 주소 Pool의 오버플로우로 정상적인 질의/응답 처리를 할 수 없게 된다.

터널링 기법중의 하나인 Teredo의 클라이언트는 최근에 통신한 상대방의 정보를 캐쉬에 저장한다. 이 점을 이용하여 악의적인 공격자는 여러 peer로 가장 다량의 패킷을 보내 클라이언트의 캐쉬에 오버플로우가 발생하도록 할 수 있다.

3.2.4 위조된 규약 메시지 전송

ISATAP 링크 내부에 존재하는 악의적인 공격자는 위조된 규약 메시지를 전송하여 자신이 ISATAP 라우터인 것처럼 가장 할 수 있다. 위조된 규약 메시지를 수신한 ISATAP 클라이언트는 자신의 PRL에 악의적인 공격자를 등록하게 된다. ISATAP 클라이언트는 PRL에 등록된 악의적인 사용자를 라우터로 착각하여 터널링 통신을 시도하게 되어 원할한 통신을 하지 못하거나 중간자공격에 이용될 수 있다.

3.2.5 소스 주소 스푸핑을 이용한 DoS 공격

혼재망과 IPv6 망 모두 IPv4와 같이 소스 주소에 대한 검증을 수행하지 않는다. 악의적인 공격자는 이를 이용 소스 주소를 스푸핑하여 특정 호스트에 DoS 공격을 수행 할 수 있다.

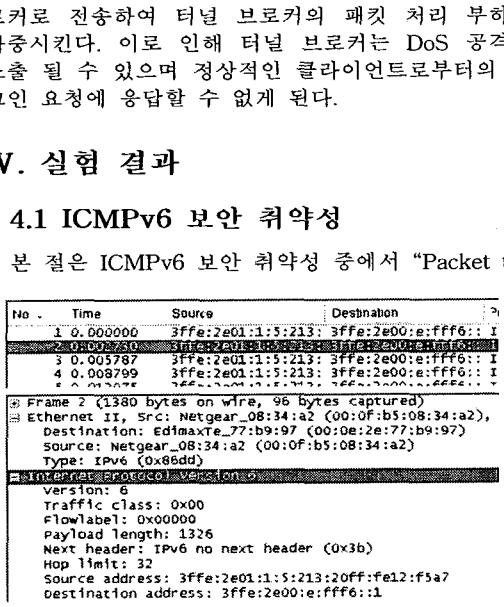
3.2.6 과다한 로그인 요청

터널링 기법중 하나인 터널 브로커[6]는 클라이언트가 신뢰성 있는 사용자임을 검증하기 위하여 로그인을 이용한 인증 작업을 수행한다. 클라이언트로 가장한 공격자는 다량의 로그인 요청 패킷을 터널 브로커로 전송하여 터널 브로커의 패킷 처리 부하를 가중시킨다. 이로 인해 터널 브로커는 DoS 공격에 노출 될 수 있으며 정상적인 클라이언트로부터의 로그인 요청에 응답할 수 없게 된다.

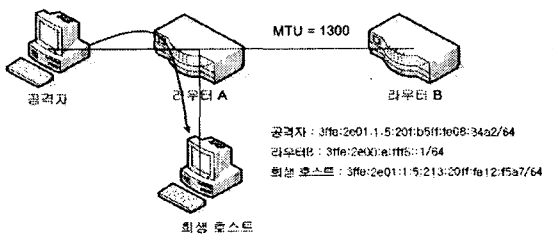
Ⅳ. 실험 결과

4.1 ICMPv6 보안 취약성

본 절은 ICMPv6 보안 취약성 중에서 "Packet too Big" 메시지를 이용한 공격 실험 내용 및 결과를 기술한다.



(그림 2) 공격자의 전송 패킷 내용



(그림 1) Packet too big 메시지 취약점 실험 환경

(그림 1)은 실험을 진행한 환경을 표현한 그림이다. 라우터A와 라우터B의 MTU는 1300으로[7] 설정이 되어 있다. IPv6에서 두 링크간에 최소한 1280이상의 MTU는 보장을 해야 한다. 실험 방법은 다음과 같다.

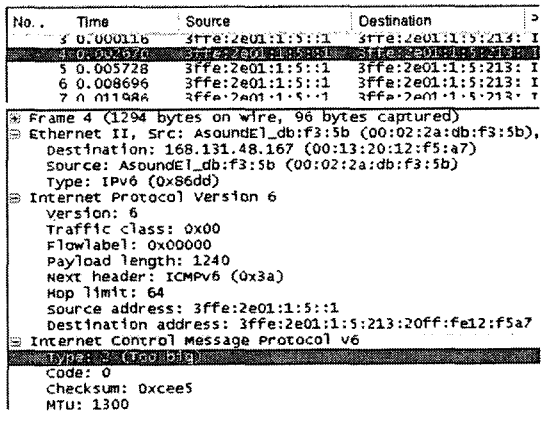
1. 공격자는 1400 바이트 크기의 패킷을 생성한다.

2. 공격자는 패킷의 소스 주소를 희생 호스트의 주소로 변경하여 라우터 B에 패킷을 전송한다.

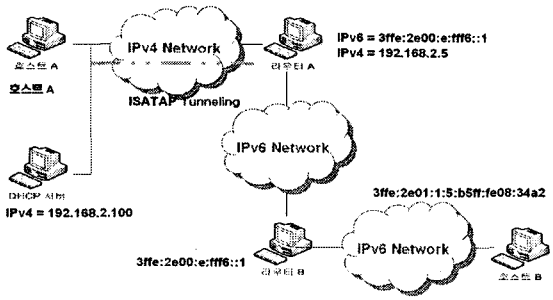
3. 위 1,2 동작을 반복한다.

위 동작의 2번에서 스푸핑 기법이 사용이 되었다. 그 이유는 공격자가 "Packet too Big" 메시지를 받으면 그 이후의 패킷은 MTU에 맞게 단편화하여 전송하게 된다. 그로 인하여 더 이상의 "Packet too Big" 메시지를 생성 할 수 없게 된다.

위 실험의 결과 공격자는 1400 바이트 크기의 패킷을 생성한다. 그리고 라우터 A는 라우터 B로 패킷을 전송하지 못하고 "Packet too Big" 메시지를 생성하여 희생 호스트에 전송한다. 희생 호스트는 "Packet too Big" 메시지에 대해 어떠한 응답 처리도 하지 않는다. 그렇기 때문에 라우터 A는 계속적으로 "Packet too Big" 메시지를 생성하여 희생 호스트에 전송할 수 있으며 공격자는 "Packet too Big" 메시지를 수신하지 못하였기 때문에 계속적으로 MTU보다



(그림 3) 희생 호스트의 수신 패킷 내용



(그림 4) ISATAP 취약점 실험 환경

큰 1400바이트 크기의 패킷을 생성 할 수 있다. 이로 인하여 공격자로부터 희생호스트까지의 경로에 대량의 트래픽이 발생 시킬 수 있었다.

4.2 ISATAP에서의 인증되지 않은 DHCP 서버

ISATAP 내부 네트워크에서 IPv4 주소를 얻기 위하여 DHCP 서버를 이용하기도 한다. 악의적인 공격자가 인증되지 않은 DHCP 서버를 운영하여 ISATAP 내부 네트워크의 호스트의 주소 구성을 방해하는 실험을 수행하였다.

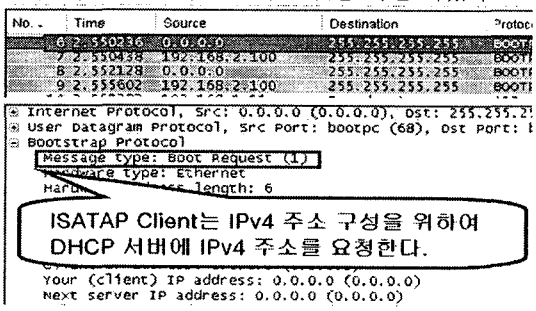
(그림 4)는 실험을 진행한 환경을 표현한 그림이다. 실험 동작 시나리오는 다음과 같다.

1. 호스트A는 ISATAP 터널링을 이용하여 호스트B와 통신하기를 희망한다. 호스트A는 현재 주소를 가지고 있지 않기 때문에 (그림 5)와 같이 동일 네트워크에 있는 DHCP 서버에 자신의 IPv4 주소를 요청한다.

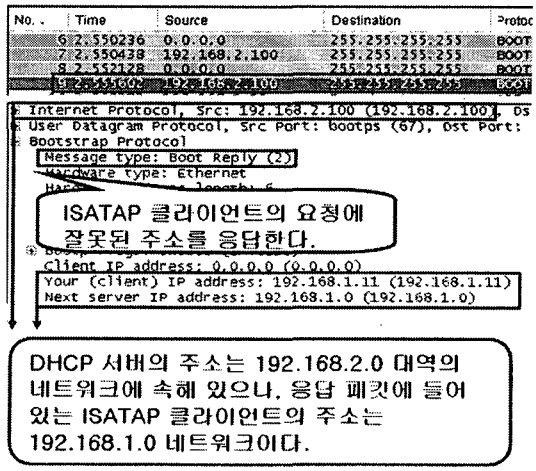
2. (그림 6)을 보면 악의적인 사용자가 가장한 DHCP 서버는 자신의 네트워크가 아닌 다른 네트워크의 IP 주소인 192.168.1.0 네트워크의 주소를 응답한다.

3. 잘못된 IPv4 주소를 구성한 ISATAP 클라이언트인 호스트A는 ISATAP 라우터인 라우터A로부터 IPv6 주소를 받아오지 못하여 원활한 통신을 수행할 수가 없게 된다.

위 실험 결과 잘못된 IPv4 주소 구성을 한 호스트는 게이트웨이를 찾지 못하여 ISATAP 라우터인 라우터A와 통신을 하지 못하는 것을 확인 하였다.



(그림 5) 호스트A의 DHCP 요청 메시지



(그림 6) 잘못된 주소 구성이 된 DHCP 응답 패킷

V. 결론 및 향후과제

IPv6에 대한 표준 논의는 마무리 되었지만, 실제 서비스에 적용하기 위해서는 미흡한 부분이 많다. 기존의 IPv4망과의 완벽한 융합이 제공되어야 하며, 사용자의 이용 편의성을 제공한다. 또한 ISP의 투자를 보호해야 하는데 그러기 위해서는 안전한 망 관리가 우선적으로 실현이 되어야 한다. 그러기 위해서는 IPv6 순수망과 IPv4/IPv6 혼재망에서의 보안 취약성에 대한 정리가 되어야 하며 그에 따른 보안 대책을 정확히 수립해야 한다. 본 논문에서는 RFC를 토대로 보안 취약성을 정리 하였으며 실험에 따른 결과를 수록하였다. 향후에는 정리된 보안 취약성에 대한 정확한 대책 수립이 필요하고, 효율적인 보안 관리를 위한 보안 프레임워크를 설계 해야 한다.

[참고문헌]

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

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

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

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

[5] 한국정보보호진흥원, IPv6 보안 기술 해설서, 2005. 10

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

[7] Darrin Miller and Sean Convery, IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0), cisco, March, 2004