유무선 IPv6 보안 위협 및 대응방안

특 집
11

목 차

신동명 · 윤미연 · 현호제 · 원유제
(한국정보보호진흥원)

1. 서 론

IPv6는 IPsec(Internet Protocol Security)을 기본적으로 제공하며 플로우 레이블을 이용한 패킷별 품질제어, 주소 자동 설정 등의 기능이 추가되어 IPv4에 비해 보안기능 및 QoS, 편리성 등의 측면이 강화되었다. 그러나 IPv6에서 제공하는 자동설정, 확장헤더 등 새로운 기능들은 공격자에 의해 악용될 수 있는 보안위협을 갖고 있다[1]. 또한, IPsec은 복잡한 설정 과정 및 키 관리 문제의 어려움 등을 가지고 있으며 모든 IPv6 보안 위협에 대한 대응방안으로 사용하기에는 부족하다.

IETF에서는 IPv6와 v6Ops[2] 워킹그룹을 중심으로 관련 그룹들과의 협력을 통하여 IPv6 보안 취약성 및 대응에 대한 표준화가 진행되고 있다. 2002년 7월, Operations and Management영역의 기존 NGTrans 워킹그룹이 새롭게 v6Ops 워킹 그룹으로 개편되었으며 62차 IETF회의에서 v6Ops 워킹 그룹을 통해 IPv4와 IPv6가 공존하는 전이 환경에서의 보안 이슈에 대한 표준화를 시작하여 현재까지 추진하고 있다. 관련 RFC로는 "Security Considerations for 6to4 (RFC 3964)"가 있으며, 드래프트 문서로는 "IPv6 Transition/Co-existence Security Considerations", "Using IPsec to Secure IPv6-in-IPv4 Tunnels", "Best Current Practice for Filtering ICMPv6 Messages in Firewalls"가 있다. IETF이외의 IPv6 보안 이슈와 관련된 작업으로 유럽의 6NET[3]에서는 "Secure IPv6 Operation: Lessons learned from 6NET", "Operational procedures for secured management with transition mechanisms" 문서를 공개하고 있다. 일본의 v6pc[4]에서도 Deployment WG의 서브 워킹 그룹인 Security SWG에서 "IPv6 Deployment Guideline"의 "security edition"으로 안전한 IPv6 운영을 위한 가이드를 제공하고 있다.

본 고에서는 MIPv6를 포함하여 표준에 명시된 IPv6의 기능들에 대한 새로운 보안 위협과 대

응방안을 기술하고, IPv4와 IPv6간의 전환에 따른 보안위협과 대응방안을 기술하기로 한다.

2. IPv6의 새로운 기능에 대한 보안 위협과 대응 방안

2.1 소스 라우팅을 위한 라우팅 헤더[5]

침입차단시스템의 필터링 규칙에 의해 공격자 A가 내부 서버 B에는 접근이 가능하나, 내부 서버 C에는 접근할 수 없도록 설정되어 있다고 가정한다. 이때 외부에서 접근이 가능한 내부 서버 B가 라우팅 헤더의 처리가 가능하고 'Segments Left' 필드 값이 1 이상인 경우에 공격자 A는 내부 서버 B를 경유하여 직접 접근할 수 없는 내부 서버 C로 공격 트래픽을 전달할 수 있다. 따라서 공격자가 라우팅 헤더를 이용하여 목적지 주소 기반의 접근 제어를 하는 침입차단시스템의 필터링을 우회할 수 있다. 대응방안으로는 호스트와 라우터에서 타입 0의 라우팅 헤더 처리를 제한하거나 침입차단시스템에서 패킷의 목적지 주소와 라우팅 헤더를 모두 비교할 수 있는 필터링 규칙을 설정하여야 한다.

2.2 사이트(Site-Local) 범위를 갖는 멀티캐스트 주소[5]

IPv6에서는 브로드캐스트 주소 대신에 멀티캐스트 주소를 이용하여 브로드캐스트 서비스를 제공한다. 또한 모든 라우터 및 DHCP를 지정하는 주소를 제공하고 있으며, 공격자는 모든 라우터를 나타내는 (FF05::2) 주소와 모든 DHCP서버를 나타내는 (FF05::3) 주소를 목적지 주소로 사용하여 내부 네트워크에 대한 스캐닝 공격 및 플러딩 공격을 할 수 있다.

대응 방안으로 외부로부터의 멀티캐스트 주소를 갖는 패킷에 대한 접근을 차단해야 하며 다음과 같은 방안을 통해서 스캔을 포함한 공격의 위험을 경감시킬 수 있다.

- 경계 라우터에서 내부용(internal-use) IPv6 주소 필터링
- 불필요한 ICMPv6 메시지의 유입 및 유출 차단
- 침입차단시스템은 최소한의 링크 로컬 멀티캐스트 주소의 트래픽만 허용(FF02::/10)
- 침입차단시스템과 경계 라우터는 사이트 범위의 목적지 주소를 갖는 패킷 유입 차단

2.3 통합 기능의 ICMPv6[6]

ICMPv6은 처리가 불가능한 특정 패킷들이 멀티캐스트 주소로 전송되면 에러 메시지를 송신자에게 응답하는 것을 허용함으로써 응답 메시지를 이용한 서비스 거부 공격과 허위 RS(Router Solicitation), RA(Router Advertisement)메시지 전송 공격 등의 보안 위협을 갖는다. 대응 방안은 침입 차단시스템에서 목적지나 목적포트에 대한 필터링뿐만 아니라 확장헤더에 대한 필터링이 가능하여야 한다. RS(Router Solicitation)와 RA(Router Advertisement)의 보안위협에 대한 대응방안으로 RFC 2461에서는 IPSec AH 이용을 제안하고 있으나, IPSec 자동 키(automatic keying) 설정의 문제로 인해 수동 키(manual keying) 설정 방식만 가능하다. 또 다른 대응방안은 SEND 워킹그룹에서 제안한 것으로 공개키 서명 방식과 CGA(Cryptographic Generated Address)를 사용하는 방식이 있다. CGA는 제공되는 보안 강도가 높고 절차가 간단하지만 각 노드에서 처리해야 하는 암호학적 연산의 양이 많아지므로 일반적으로 성능이 낮은 이동 단말에서는 적용하기 어렵다.

2.4 최적의 서비스 탐색을 위한 애니캐스트

애니캐스트 서비스에서 송신자의 요청은 애니캐스트 라우터를 통하여 짧은 홉거리, 낮은 비용, RTT 등을 고려하여 적합한 그룹의 멤버에게 전달되며, 이때 그룹 멤버는 응답 메시지의 소스주소를 글로벌 유니캐스트 주소로 송신자에게 응답한다. 이때의 보안 위협은 인증되지 않은 애니

캐스트 그룹 멤버가 거짓 응답 메시지를 전송하여 위장공격(Masquerading)을 하거나 정상 서비스를 방해할 수 있다. 대응방안으로 인증되지 않은 애니캐스트 요청을 필터링하거나 IPSec을 애니캐스트에 적용하여 보안채널을 사용할 필요가 있다.

2.5 동적 주소설정을 위한 프라이버시 확장[7]

프라이버시 확장(privacy extensions)은 인터페이스 식별자를 변경하여 호스트의 IPv6주소가 스캔 위협에 노출되는 것을 방지하는 목적으로 사용된다. 반면에 공격자의 인터페이스 식별자 변경이 용이하여 침해사고 시 공격자에 대한 추적 및 호스트의 관리가 어려워질 수 있다.

호스트가 주소를 할당 받기 위해 수동설정이나 DHCP를 이용하는 경우에는 DNS에 주소를 등록하는 것이 제한적이나 주소 자동 설정을 이용하면 DDNS(Dynamic DNS)를 통해 동적으로 주소를 등록할 수 있다. 이때 공격자는 과도한 DDNS 업데이트 요청을 통해 서버의 가용성 문제를 발생시킬 수 있다. 대응방안으로 주소 설정을 위한 노드와 DDNS 서버 간 SA(Security Association)를 통하여 인증된 노드만이 주소 갱신을 하도록 하고 프라이버시 확장을 사용하는 노드는 주소 업데이트 주기에 대한 적절한 값을 설정해야 한다.

2.6 IPv6 주소 및 포트 정보를 이용한 접근제어

IPv6 기반의 침입차단시스템은 접근제어 기능을 사용하여 인증된 호스트만 내부 네트워크로 접속할 수 있게 한다. 그러나 IPv6 노드는 다중 주소를 가질 수 있기 때문에 다중 주소와 라우팅을 고려한 보안 정책이 필요하다.

IPSec 터널링을 이용하는 경우 IPv6 메시지가 암호화 되어 전송되기 때문에 메시지의 내용을 확인할 수 없어 필터링의 적용이 곤란하며 공격자는 이를 악용하여 공격패킷을 암호화하여 전송함으로서 침입차단시스템을 통과할 수 있는 위협이 있다.

대응방안으로 IPv6는 하나의 인터페이스에 다중 주소가 허용되므로 침입차단시스템에서는 글로벌 주소에 대해서는 허용하고, 링크 로컬 주소에 대해서는 외부로 나가는 것과 외부에서의 접근을 막아야 한다. 또한, 호스트에서 침입차단 시스템을 이용하여 암호화된 패킷에 대한 필터링 기능을 제공할 필요가 있다.

2.7 전송 패킷의 단편화(Fragmentation)

IPv6에서는 단편화 과정이 IPv4와는 달리 단말 호스트에서만 이루어진다. 이러한 점을 악용하여 공격자가 단편화 패킷의 일부를 중복 전송하는 경우 최종 목적지의 호스트는 분할된 패킷의 재조합(reassembly)시 중복된 단편화 패킷 중 어떤 패킷이 올바른 것인지 판단할 수 없게 된다. 이로 인해 시스템이 교착 상태에 빠지거나, 불법 권한획득의 문제를 가질 수 있다. 대응 방안으로는 침입차단시스템이 단편화 패킷을 재조합하여 필터링을 적용하는 방법등을 고려해 볼 수 있다.

3. MIPv6 기술의 보안 위협과 대응 방안

MIPv6 (Mobile Internet Protocol version 6)는 인터넷 사용자가 이동 중에도 끊김 없는 서비스를 제공받을 수 있도록 하는 IPv6 프로토콜이다. MIPv6는 이동사용자의 핸드오프 과정을 정의하고 있으며, 핸드오프시 발생할 수 있는 보안위협에 대응할 수 있는 보안기법을 제시하고 있다.

3.1 MIPv6의 개요

MIPv6는 IPv6에 이동성을 제공하기 위한 프로토콜 세 가지의 구성요소를 갖는다. 이동노드인 MN(Mobile Node), 이동노드의 홈에이전트인 HA(Home Agent) 그리고 통신 대상개체인 CN(Correspondant Node)으로 구성된다.

이동노드 MN은 자신의 홈네트워크에서 CN으

로부터 데이터를 전달 받으며 외부 네트워크로 이동시에는 라우팅 최적화 과정을 통해 옮겨진 외부 네트워크로 데이터를 전달받는다. 외부네트워크로 이동한 MN이 해당 네트워크에서 CoA (Care of Address)를 획득하고, BU(Binding Upate)메시지를 통해 CoA를 HA와 CN에게 알린다. CN 과 HA는 CoA로의 바인딩 캐시를 갱신 후 MN에게 BA메시지를 보냄으로써 갱신과정을 마치고 CN에서 MN까지 새로운 CoA를 목적지 주소로 하여 패킷이 전달된다[8].

3.2 MIPv6에서의 보안위협

먼저 MIPv6는 기본 IPv6 기능의 확장이기 때문에 데이터 보안의 측면에서 적어도 기본 IPv4 또는 IPv6 만큼의 보안성을 제공할 수 있어야 하며 IPv6에 대한 새로운 보안취약성을 만들지 않아야 한다. 그러나 이동성 지원시 사용되는 바인딩 메시지들을 이용하여 새로운 보안 취약점이 발생할 수 있다. 이러한 취약점을 보완하기 위하여 MIPv6 표준에서는 기본적으로 바인딩 메시지들에 대한 인증 절차를 제시하고 있다. 본 절에서는 바인딩 메시지들의 인증절차를 수행하지 않았을 때에 발생할 수 있는 보안위협에 대하여 알아보도록 한다. <표 1>과 같이 MIPv6의 바인딩 업데이트 메시지, 홈어드레스 옵션, 라우팅 헤더, 터널링 등에 의해 보안취약성이 발생할 수 있으며 이를 이용하여 서비스 거부공격, 중간자 공격(Man-in-the-middle Attack), session hijacking, 위장 공격 등이 가능하다.

터널링 및 라우팅헤더를 이용시에 가질 수 있는 취약성은 유선망에서도 공통적이다. 그러나, 바인딩 업데이트와 홈어드레스 옵션(HAO) 사용시의 취약성은 이동 환경에서만 발생한다.

MN은 CN과 통신할 때 패킷의 소스 주소로 자신의 CoA를 사용하고 HAO(Home Address Option)에 자신의 HoA(Home Address)를 넣어서 전송한다. 이를 수신한 CN은 소스 주소와 HAO 내의 주소를 교체하여 사용한다. 이 때, 보안취약성을 이용한 위협요소로는 이동단말이 바인딩 업데이트 메시지를 HA로 전송할 때와 CN으로 전송할 때로 나눌 수 있다. MN이 BU 메시지를 HA로 전송할 때, 공격자는 MN에 대해 현재 위치한 곳과 다른 곳에 위치해 있다는 정보를 줄 수 있고, HA가 이 정보를 받아들인다면, MN은 패킷을 받지 못하는 반면 다른 노드가 원하지 않는 패킷을 수신한다.

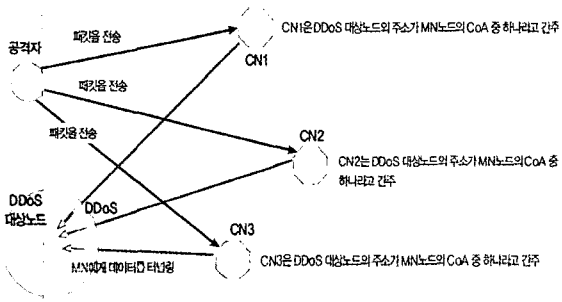
<표 1> MIPv6의 보안취약성

구분	보안취약성
바인딩 업데이트	홈에이전트로의 바인딩 업데이트 메시지에 대한 취약성
	CN과의 라우팅 최적화에 대한 취약성
	MIPv6 CN의 기능이 다른 노드로의 반사 공격의 시발점으로 사용될 수 있는 취약성
홈어드레스 옵션	보안 기법들을 위한 고비용의 암호알고리즘들을 불필요하게 실행시키도록 하는 등의 공격을 받을 수도 있음
라우팅헤더	MIPv6를 사용하는 IPv6 헤더가 침입차단시스템상의 규칙에 기반한 IP주소를 우회하거나 다른 노드들로부터 트래픽을 반사시키는 데 사용될 취약성
터널링(IP헤더)	이동노드와 홈에이전트간의 터널에 이동노드가 트래픽을 보내는 것처럼 보이게 하는 공격으로 인한 취약성

또한, CN으로 BU 메시지를 전송할 때 공격자가 자신의 HoA를 희생자의 HoA로 설정하여 거짓 정보를 알릴 경우, CN에서 희생자로 전송하고자 하는 패킷은 공격자를 거치게 되므로 가용성과 기밀성을 모두 위협한다. 또한 공격자가 자신의 CoA를 거짓으로 알리는 경우, CN은 이동단말로 보내는 패킷을 모두 거짓 CoA로 전송하여 서비스 거부 공격을 할 수 있다. 그리고 CN으로 의미 없는 BU 메시지를 한꺼번에 많이 전송할 경우에는 CN에서 그 메시지가 유효하지 않음을 알아채기 전에 자원을 고갈시켜 의미 있는 패킷들을 처리할 수 없게 만든다. 마지막으로 공격자는 오래된 BU 메시지를 재실행하여 패킷들을 MN의 예전 위치로 전달시켜 MN이 패킷을 수신하지 못하게 만들 수 있다.

HAO를 사용할 경우 발생할 수 있는 보안상의

취약성은 공격자가 HAO를 사용하여 서비스거부공격을 할 수 있다는 것이다. 공격자는 (그림 1)에서와 같이 보낼 패킷의 HAO필드 홈주소를 넣고 소스주소 부분에 희생자의 주소를 넣어 보내면 CN노드는 그 주소로 응답을 보내게 되어 실제 희생자 노드에게 서비스 거부 공격을 행할 수 있다. 또한 이는 희생자들이 불필요하게 고비용의 암호알고리즘들을 실행하도록 한다. MIPv6에서 희생자는 이러한 경우에 정상적인 IPv6 동작을 하는 과정까지 모든 암호화 알고리즘 처리를 중지할 수도 있다.



(그림 1) HAO를 이용한 DDoS공격 예시

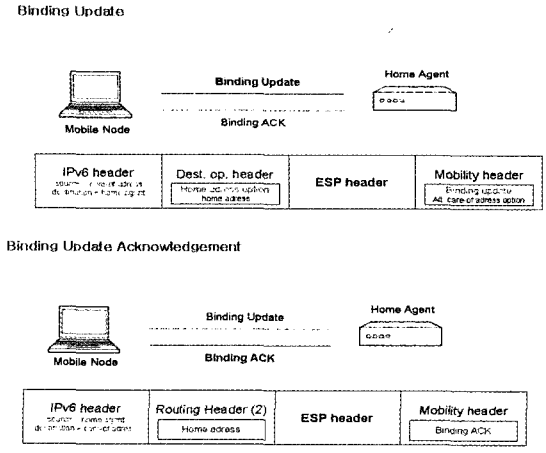
또한 BA메시지에 사용되는 라우팅헤더는 기존의 MIPv6에서 사용하도록 한 Type 0의 라우팅 헤더를 사용시 호스트나 라우터에서 모두 처리 가능하여, 여러 개의 주소를 담아서 전송될 수 있기 때문에 반사 공격(reflection attack)에 이용될 수 있다.

마지막으로 HA와 MN간 터널의 부적절한 사용은 보안취약성이 될 수 있다. 만약 알 수 없는 노드가 터널링된 패킷 내부헤더상의 희생자 노드 MN의 목적지주소 부분에는 거짓주소를 포함하여 HA에게 보낸다면 HA는 해당 패킷을 MN에게 전달한다. 이 또한 서비스거부공격에 사용될 수 있으며 수신한 노드들에게 불필요한 보안 알고리즘을 수행하여 많은 컴퓨터자원을 소모시킬 수 있다.

3.3 MIPv6에서의 대응방안

MIPv6 표준에서는 이러한 보안취약성에 대응하기 위하여 메시지들의 인증절차를 정의하고 있다. HA와 MN간에는 사전에 SA(Security Association)이 맺어져야 하며, 이를 기반으로 하여 IPSec(IP Security)의 Transport모드로 ESP (Encapsulation Security Payload)헤더를 이용하여 BU, BA(Bingding update Acknowledgement) 및 BR(Binding update Request) 메시지 인증을 수행한다. 또한, MN과 CN사이에는 사전에 SA를 맺기가 어렵기 때문에, RR(Return Routability) 기법을 적용하여 BU, BA 및 BR 메시지의 인증을 통해 바인딩 업데이트 및 HAO 옵션의 취약점을 해결할 수 있다. (그림 2)는 HA와 MN이 바인딩 업데이트를 위해 교환하는 메시지들의 헤더부분을 나타낸 것으로 바인딩 업데이트(Binding Upadate)메시지의 헤더 부분에서 목적지 옵션 헤더(Destination Option Header)에 포함되는 "Home address"는 미리 협약된 SA를 확인하는데 사용되며, ESP Header를 붙여서 MN BU메시지를 수신시 검증할 수 있도록 한다. 또한 BA메시지의 헤더 부분에서 라우팅 헤더(Routing Header)에 "Home address"를 넣는 것은 SA를 확인하기 위해서이며, "Binding Ack" 부분은 암호화되고 , ESP헤더를 붙임으로서 이를 수신한 HA가 메시지를 검증할 수 있도록 하였다. 여기서 라우팅 헤더는 소스 라우팅에서 사용되는 것과 구별하여 소스 라우팅으로 인한 보안취약점을 방지하기 위해 라우팅 헤더를 사용하지 못하도록 할 경우에도 MIPv6가 정상동적을 할 수 있도록 type 2로 정의하여 사용된다.

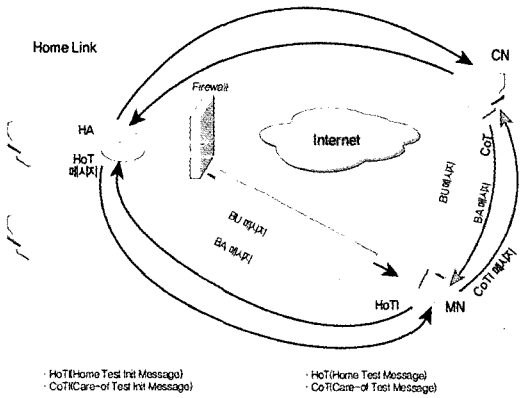
(그림 3)은 MN과 CN사이의 바인딩 업데이트 메시지들의 인증을 위해 사용되는 RR절차를 나타낸 것이다. 먼저 MN이 쿠키정보를 담은 HoTI 메시지를 HA를 경유하여 CN에게 보내고, CoTI를 CN에게 보낸다. 이를 수신한 CN은 임의로 생



(그림 2) HA와 MN사이의 바인딩 업데이트 메시지 인증

성한 키를 이용하여 HMAC_SHA1 알고리즘에 홈주소, HoA 넌스 정보 등을 입력으로 한 출력 값의 처음 64비트만을 잘라내어 Home Keygen Token을 생성하고, 마찬가지 방법으로 CoA와 CoA Nonce정보 등을 입력으로 하여 Care-of Key Token를 생성하여 MN에게 각각 HoT 및 CoT메시지에 실어서 보내준다. CN는 이후 두 토큰 정보를 이용하여 인증에 사용될 킷값을 생성하며, 이 두메시지를 수신한 MN 또한 이를 이용하여 메시지 인증에 사용될 키 값을 유도한다. 이후, MN은 인증키를 이용하여 BU메시지의 인증정보를 생성하고 이와 함께 BU를 CN에게 보내고, CN은 마찬가지로 인증정보와 함께 BA를 보냄으로써 검증된 바인딩 업데이트 메시지들의 교환이 이루어지도록 한다. 이를 이용하여 BU 메시지의 위변조를 통한 보안위협에는 대응할 수 있도록 하였다. 그러나 IPv6 주소 자체의·검증은 불가능하므로 향후 CGA(Cryptographically Generated Address)[9] 기법을 이용하여 이에 대한 검증이 가능할 것으로 기대된다.

BA메시지의 라우팅 헤더의 사용으로 인한 보안위협에 대응하기 위해서는 MIPv6에 기존의 라우팅 헤더를 사용하지 말고 새로운 목적지 옵션, 새로운 확장 헤더 또는 새로운 라우팅 헤더 타입을 정의하여 사용하는 것으로 이를 위해 Type 2의 라우팅 헤더가 새로이 정의되어서 보안 취약성에 대응한다. 그 외에 대응방안은 라우팅 헤더 자체를 안전하게 사용하는 것이다. 즉, 호스트나 내부 라우터들은 라우팅 헤더를 처리하여 전송할 수 없도록 하는 것이다. 이 방법은 모든 호스트와 라우터에서 라우팅 헤더를 처리하여 전송하는 것을 제한하기 때문에 초기에 의도한 라우팅 헤더의 목적으로 사용할 수 없고, MIPv6에서만 유용하게 사용되는 단점이 있다. 그리고 침입차단시스템의 기능을 강화하는 것으로 이 방



(그림 3) MN과 CN사이에서의 RR 동작 개요

법은 침입차단시스템에서 MIPv6는 지원하면서 차단에 필요한 규칙을 사용하자는 것인데, 이 방법은 침입차단시스템의 규칙이 복잡해지고 강화된 필터링으로 인해서 경로 최적화에 실패하는 경우도 발생할 수 있는 문제점이 있다.

마지막으로 HA에 의해 CN의 패킷을 MN으로 전달하는 경우에 터널링으로 인해 발생할 수 있는 보안위협은 HA가 패킷을 전달하기 전에 수신한 터널링된 패킷의 내부 및 외부 IP헤더상의 소스 주소들이 유효한 바인딩인지 검증함으로써 이를 방지할 수 있다.

4. IPv4/IPv6 전환기술의 보안 위협과 대응 방안

IPv4 망에서 IPv6 망으로의 전환(Transition)

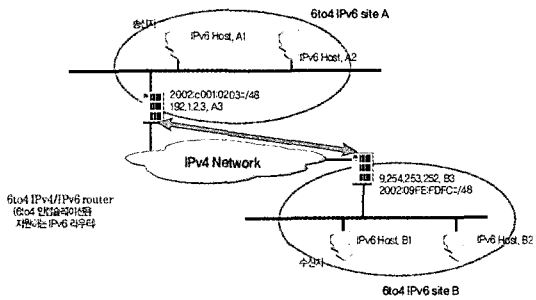
기술로는 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation)이 있다. IPv6 호스트가 IPv4 호스트와 호환성을 유지하는 가장 쉬운 방법은 IPv4/IPv6 듀얼 스택을 제공하는 것이다. 이때의 호스트는 IPv4와 IPv6 각각에 대한 보안위협에 대해 대응방안을 마련해야 한다.

IPv4/IPv6 변환기술은 IPv4 네트워크와 IPv6 네트워크간의 통신을 위해 중간에 변환기를 사용하는 방식이다. IPv4/IPv6 변환은 네트워크/전송/응용 계층에서 수행될 수 있고, 변환을 수행하는 계층이 상위일수록 호환성은 좋아지나 성능이 저하된다. 네트워크 계층에서의 변환을 수행하는 방법으로 NAT-PT/NAPT-PT (Network Address Translation-Protocol Translation /Network Address Port Translation-Protocol Translation)가 있다. NAT-PT와 NAPT-PT는 IPv4 패킷을 IPv6 패킷으로 혹은 그 반대로 변환시켜 주는 기능을 한다. 그러나 NAT가 일대일로 IP 주소를 변환하는 것에 비해 NAPT는 다대일로 IP 주소를 변환시키고 포트번호를 통하여 구분하는 기능을 갖는다. 이때의 보안위협으로 NAT-PT 장비에 장애가 발생하거나 장애를 유발시켜 서비스가 중단된 경우, 공격자가 IPv6 호스트에 조작된 IPv6 프리픽스를 할당하여, IPv4 호스트로 전달될 모든 패킷을 가로챌 수 있다. 또한 NAT-PT 장비가 위치한 네트워크에서 공격자가 스푸핑된 패킷을 IPv4 네트워크로 다량 전송하면, 주소풀(Address Pool)에 등록된 IPv4 주소를 고갈시켜 서비스거부공격이 가능하다. 이러한 보안취약성에 대한 대응방안으로는 NAT-PT 에서 인그레스 필터링을 통해 소스 주소의 위조를 탐지하여 차단하고, NAT-PT 게이트웨이는 필터링을 통해 IPv4 소스 주소가 브로드캐스트/멀티캐스트 주소인 모든 패킷들을 폐기함으로써 서비스거부공격을 방지할 수 있다.

IPv4/IPv6 터널링 방식으로는 IPv6-in-IPv4, 6to4, ISATAP, 터널 브로커 활용 터널링, DSTM, Teredo 터널링 등 다양한 방식이 있다. 일반적으로 터널링 방식에서는 네트워크를 보호하기 위해 설치된 침입차단시스템이나 침입탐지시스템을 우회할 수 있으며 서비스 거부 공격이나 주소 스푸핑 공격에 노출되어 있다.

4.1 6to4 터널링[10]

6to4 터널링 방식은 IPv6 주소에 IPv4 주소를 삽입하여 IPv4 망에서는 IPv4 패킷으로 라우팅 처리되고 IPv6 망에서는 IPv6 패킷으로 라우팅 처리되는 터널링 기술로 확장성이 뛰어나다(그림 4).



(그림 4) 6to4의 동작

6to4 호스트들은 공격자가 조작한 IPv4 in IPv6 트래픽과 6to4 릴레이 서버로부터 수신한 트래픽을 구분하지 못한다. 따라서 IPv6 노드에 대한 소스 주소 스푸핑과 DRDoS(Distributed Reflection of Denial-of-Service) 공격 모두에 노출되어 있다. 또한 공격자인 IPv6 노드가 자신의 실체를 숨기는 수단으로써 릴레이 서버를 이용할 수 있다. 즉, 공격자는 터널링된 패킷을 스푸핑하여 IPv4 호스트를 공격할 수 있다. 대응 방안으로 관리자는 서로 다른 6to4 주소 간에는 릴레이하지 않도록 6to4 릴레이 서버를 설정해야 하며 6to4 릴레이는 6to4 주소의 유효성을 검증할 필요가 있다. 즉, 6to4 주소내의 IPv4 주소가 글로벌 유니캐스트 주소이고, 실제 사용되는 주소인지를 검증해야 한다.

4.2 ISATAP(Intra Site Automatic Tunnel Address Protocol) 터널링

ISATAP는 IPv4 네트워크 내부에 존재하는 듀얼스택 호스트가 IPv6 호스트와 통신을 하기 위한 방법으로 IPv4 터널링을 위한 별도의 라우터가 필요하다.

ISATAP를 이용하면 터널이 사용되므로, 캡슐화된 IPv6 패킷의 악성 여부를 판별하기 어렵다. 또한, ISATAP 라우터의 사용자 인증기능이 없는 경우 공격자가 해당 ISATAP 라우터의 주소만 알아내면 터널을 사용할 수 있다는 취약점을 갖는다.

대응 방안으로 ISATAP 서버나 라우터는 내부 호스트들이 요청한 터널만을 정당한 것으로 인식하여야 한다. 이러한 접근제어는 침입차단시스템을 이용하여 설정할 수 있다. 단, 침입차단시스템의 ACL을 설정할 때, IPv4 경계 라우터는 프로토콜타입 41(IPv6-in-IPv4 트래픽)을 허용하도록 설정해야 한다. 또한, ISATAP 서버의 정보가 DHCP 등을 통해 외부로 유출 되지 않도록 장비를 설정해야 하며, RA나 ND(Neighbor Discovery)메시지를 통한 정보 유출을 차단해야 한다.

4.3 터널 브로커(Tunnel Broker) 활용 터널링

IPv6 네트워크에 안정적이고 지속적인 IPv6 주소와 도메인 네임을 전달하기 위해 도입된 개념으로서 터널 브로커라는 전용 서버를 구축하여 사용자의 터널링 요구를 자동으로 관리하는 방법이다.

일부 터널 브로커 서비스는 사설 IPv4 환경에서도 IPv6 주소체계를 이용할 수 있는 NAT 기능을 지원하고, 터널 설정을 위한 프로토콜(TSP: Tunnel Setup Protocol)을 사용할 수 있는 전용 클라이언트를 제공하기도 한다. 그러나 터널 브로커 사용자에 대한 적절한 인증 절차가 없다면, 보안위협이 발생할 수 있다. 특히, 악의를 가진 공격자가 터널의 설정을 임의로 변경하면, 불법적으로 네트워크에 접근하거나 서비스 거부공격을 유발할 수 있다. 또한, 세션에 대한 관리가 부적절하다면, 공격자가 다른 사용자의 세션을 가로챌 수 있다. 이러한 보안위협은 사용자별로 정적으로 IP주소를 할당하는 서비스에서 보다 동적으로 IP주소를 할당하는 서비스에서 발생하기 쉽다.

이러한 위협에 대응하기 위해 관리자는 터널 브로커 서비스를 사용하는 사용자에 대한 인증 메커니즘을 구축·운영하여야 한다. RFC3129에서는 사용자에게 Kerberos 티켓을 발행하는 메커니즘이 제시되어 있다. 터널 양단의 네트워크 주소를 파악하여 패킷의 소스나 목적지 주소가 위조된 경우 판별하기 위해서는 관리자는 터널에 대한 필터링 정책을 적용해야 한다.

5. 결 론

기존 IPv4 프로토콜은 보안을 고려하여 설계하지 않았기 때문에, 다양한 보안공격에 노출되어 있는 반면에 IPv6에서는 IPsec을 기본으로 제공하고 있기 때문에 다양한 공격을 상당부분 해결할 수 있다. 그러나, IPv6에서 제공하는 자동설정, 확장헤더 등 새로운 기능들은 공격자에 의해 악용될 수 있는 보안취약성을 갖고 있다. 대부분의 사람들이 IPv6의 보안을 위한 기술로 IPsec만을 국한하고 있지만 복잡한 설정 및 키관리 문제의 어려움 등을 가지고 있으며 모든 IPv6 보안공격에 대한 대응방안으로 사용하기에는 부족하다. 또한 이동노드의 핸드오프시 HA(Home Agent) 및 CN(Correspondent Node)와의 바인딩 업데이트 절차시 발생할 수 있는 보안위협 및 IPv4 망에서 IPv6 망으로의 전환과정에 따른 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation) 방식에서의 보안위협 등에 대응하기 위한 지속적인 보안기술 개발 및 보안 솔루션의 운영을 통한 사전예방 활동이 중요하다.

참고문헌

[1] E. Davies, S. Krishnan, P. Savola. "IPv6 Transition/Co-existence Security Considerations," IETF Draft, draft-ietf-v6ops-security-overview-03.txt. October 6, 2005

[2] IPv6 Operation WG (v6ops), http://www.ietf.org

[3] "large-scale international IPv6 pilot network," http://www.6net.org/.

[4] "IPv6 promotion council," http://www.v6pc.jp/

[5] S. Deering, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, IETF, 1998

[6] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC 2463, IETF, 1998.

[7] "Privacy Extensions for Stateless Address auto-configuration in IPv6," RFC 3041, 2001

[8] D. Johnson, "Mobility Support in IPv6", RFC 3775, June 2004.

[9] Aura. T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[10] P. Savola, "Security Considerations for 6to4," RFC 3964, IETF, 2004

[11] "DSTM(Dual Stack Transition Mechanism)," http://www.dstm.info/

[12] "Review of IPv6 Transition Scenarios for European Academic Networks," IPv6 Conference, 2002

[13] "Unmanaged Networks IPv6 Transition Scenarios," RFC 3750

[14] "A Discussion on IPv6 Transition Mechanisms," IPv6style in Japan, 2003

[15] "Security and IPv6," http://www.ipv6.bt.com/tutorials/security.html

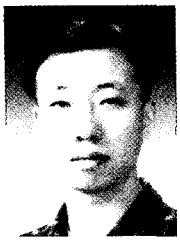
저자약력

신 동 명

2000년 2월 대전대학교 컴퓨터공학과 공학석사
2003년 8월 대전대학교 컴퓨터공학과 공학박사
2001년 7월- 현재 한국정보보호진흥원 응용기술팀 선임연구원
관심분야 : 멀티캐스트 보안, 소프트웨어 보안 취약성 분석, IPv6 보안 등
이 메 일 : dmshin@kisa.or.kr

윤 미 연

2002년 2월 숭실대학교 컴퓨터학과 공학석사
2005년 8월 숭실대학교 컴퓨터학과 공학박사
2005년 6월- 현재 한국정보보호진흥원 응용기술팀 선임연구원
관심분야 : IPv6 보안, 멀티캐스트 보안, 센서네트워크 보안
이 메 일 : myyoon@kisa.or.kr



현 호 재

1999년 2월 건국대학교 컴퓨터공학과 공학석사
2005년 8월 건국대학교 컴퓨터공학과 공학박사
2005년 2월 ~ 2006년 4월 : 한국정보보호진흥원 정보보호기술단 위촉연구원
관심분야 : 멀티캐스트 보안, IPv6 보안, 홈 네트워크 미들웨어, QoS 등
이 메 일 : dreamii@empal.com

원 유 재

1987년 충남대학교 전산학과 공학석사
1998년 충남대학교 전산학과 공학박사
1987년 ~ 2001년 한국전자통신연구원 팀장
2001년 ~ 2004년 안랩유비웨어 연구소장
2004년- 현재 한국정보보호진흥원 응용기술팀 팀장
관심분야 : IPv6 보안, 멀티캐스트 보안, 무선 인터넷 보안, PKI 등
이 메 일 : yjwon@kisa.or.kr