情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

IPv6 보안 위협 및 대응 방안

신 동 명*, 현 호 재*, 윤 미 연*, 원 유 재*

요 약

IPv6 보안의 특징은 늘어난 주소공간으로 자동화된 스캐닝과 웜 전파가 어려워지고, 링크로컬 주소의 사용으로 외부공격자의 내부네트워크 접근이 제한되고 IPsec을 기본적으로 제공하는 등 향상된 부분이 있는 반면에 IPv6 운용 및 관리 부주의로 인한 보안위협 및 공격자의 위장, 메시지 변조, 오남용 등 적극적인 공격에는 여전히 노출되어 있다. 또한 IPv4와 IPv6가 혼재하는 구간에서는 IPv4와 IPv6 각각의 보안위협뿐만 아니라 패킷 변환과정에서 나타날 수 있는 보안위협까지 고려해야 한다. 본고에서는 IPv6 표준에 명시된 기능들에 대한 새로운 보안 위협과 대응방안을 정리하며, IPv4와 IPv6간의 전환에 따른 보안위협과 대응방안을 기술한다.

Ⅰ. 서 론

기존 IPv4 네트워크 환경에서는 보안을 고려하여 설계하지 않았기 때문에, 다양한 보안공격에 노출되어 있으며, 이를 해결하기 위하여 IPv6에서는 IPsec을 기본적으로 제공하고 있다.

그러나 IPv6에서 제공하는 자동설정, 확장헤더 등 새로운 기능들은 공격자에 의해 악용될 수 있는 보안 위협을 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. IETF이외의 IPv6 보안 이슈와 관련된 작업은 유럽에서의 6NET[3], 일본의 v6pc[4], 미국의 CISCO[5]등 국내외에서 이루어지고 있다.

본 고에서는 먼저 IPv6 표준에 명시된 기능들에 대한 새로운 보안 위협과 대응방안을 기술하고, IPv4와 IPv6간의 전환에 따른 보안위협과 대응방안을 기술하기로 한다.

Ⅱ. IPv6 표준 기능의 보안 위협과 대응 방안

패킷의 무결성 및 기밀성은 IPv6상에서 기본적으로 제공하는 IPSec을 이용하여 제공할 수 있다. 그러나 IPv4에서의 보안 위협인 스니핑, 응용계층에서의 공격, Rogue 디바이스, 중간자(Man-In-The-Middle)공격, 플러딩 공격들은 IPv6 에서도 가능하며 ICMPv6, 라우팅헤더, 프라이버시 확장, 패킷단편화 등 IPv6에서 추가되거나, 변경된 방식에 대한 새로운 보안위협이 존재한다.

본 절에서는 IPv6의 새로운 기능에 대해서 공격자의 주소위장, 메시지 변조 등 적극적인 공격이나 조작에 의한 보안 위협들을 기술하고 그 대응 방안을 기술한다.

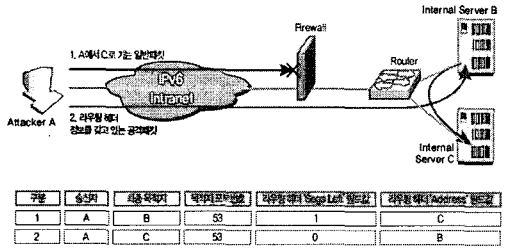
2.1 소스 라우팅을 위한 라우팅 헤더[6]

침입차단시스템의 접근제어 규칙에 의해 공격자 A가 내부 서버 B에는 접근이 가능하나, 내부 서버 C에는 접근할 수 없도록 설정되어 있다고 가정한다.

이때의 위협은 그림 1과 같이 외부에서 접근이 가

* 한국정보보호진흥원 (dmshin, hjhyun, myyoon, yjwon@kisa.or.kr)

능한 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. 대응방안은 호스트와 라우터에서의 타입 0의 라우팅 헤더 처리를 제한하거나 금지 시키고 firewall에서 패킷의 목적지 주소와 라우팅 헤더를 비교할 수 있는 필터링 규칙을 설정하여야 한다.



〔그림 1〕 라우팅 헤더 보안 취약성

2.2 사이트(Site-Local) 범위를 갖는 멀티캐스트 주소[6]

IPv6에서는 브로드캐스트 주소 대신에 멀티캐스트 주소를 이용하여 브로드캐스트 서비스를 제공한다.

〔표 1〕 사이트 범위 멀티캐스트 주소

사이트 범위를 갖는 멀티캐스트 주소	의 미
FF05::2	모든 라우터를 지칭
FF05::3	모든 DHCP 서버를 지칭

표 1과 같이 모든 라우터 및 DHCP를 지정하는 주소를 제공하고 있으며, 공격자는 모든 라우터를 나타내는 (FF05::2) 주소와 모든 DHCP서버를 나타내는 (FF05::3) 주소를 목적지 주소로 사용하여 플러딩 공격(Flooding Attack)을 할 수 있다.

대응 방안으로 외부로부터 멀티캐스트 주소에 접근할 수 없도록 네트워크 경계 지역의 침입차단시스템 및 침입탐지시스템에서 필터링을 수행하여야 한다. 또한 다음과 같은 방안을 통해서 스캔을 포함한 공격의 위험을 경감시킬 수 있다.

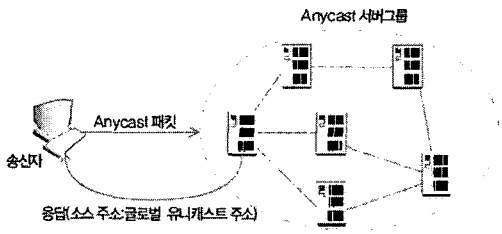
- 경계 라우터에서 내부용(internal-use) IPv6 주소 필터링
- 주요 시스템에는 추측이 어려운 IPv6 주소 할당 사용
- 불필요한 ICMPv6 메시지의 유입 및 유출 차단
- 침입차단시스템은 최소한의 링크 로컬 멀티캐스트 주소의 트래픽만 허용(FF02::/10)
- 침입차단시스템과 경계 라우터는 사이트 범위의 목적지 주소를 갖는 패킷 유입 차단
- 노드가 사이트 범위 내의 적법하지 않은 멀티캐스트 그룹에 가입 방지

2.3 통합 기능의 ICMPv6[7]

ICMPv6은 처리가 불가능한 특정 패킷들이 멀티캐스트 주소로 전송되면 에러 메시지를 송신자에게 응답하는 것을 허용함으로써 응답 메시지를 이용한 서비스 거부 공격과 RS(Router Solicitation), RA(Router Advertisement)메시지에 대한 위변조 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 RFC2461[1]에서는 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

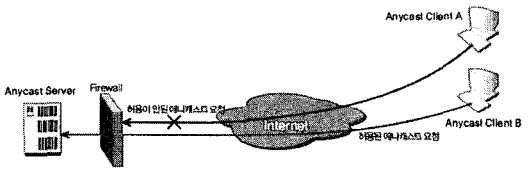


〔그림 2〕 애니캐스트를 이용한 통신

1) Neighbor Discovery for IP Version 6 (IPv6)

그림 2와 같이 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 변경하여 송신자에게 응답한다. 이때의 보안 위협은 인증되지 않은 애니캐스트 그룹 멤버가 거짓 정보를 광고하거나 해당 멤버에 의해 송신자의 주소를 변경할 수 있는 보안취약성으로 인하여, 위장공격(Masquerading) 및 서비스거부공격이 가능하다. 대응방안은 그림 3과 같이 외부에서의 애니캐스트 서비스 요청을 제한하기 위해 침입차단시스템은 사용되는 애니캐스트 주소를 필터링을 해야 한다.

또는 IPSec 및 IKE(Internet Key Exchange protocol)를 애니캐스트에 적용하여 보안채널을 사용해야 한다.



〔그림 3〕 침입차단시스템을 이용한 패킷 필터링

2.5 동적 주소설정을 위한 프라이버시 확장[8]

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. 이로 인해 공격자가 자신의 주소를 용이하게 변경할 수 있어 분산서비스거부공격의 위협이 될 수 있다. 또한 주소 자동 설정에 프라이버시 확장을 사용하면 DDNS의 업데이트 작업의 빈도를 증가시켜 서버의 가용성 문제를 발생시킬 수 있다.

이를 해결하는 방안은 주소 설정을 위한 노드와 DDNS 서버 간 SA(Security Association)를 통하여 인증된 노드만이 주소 갱신을 하도록 하며 프라이버시 확장을 사용하는 노드는 주소 업데이트 주기에 대한 적절한 값을 설정해야 한다.

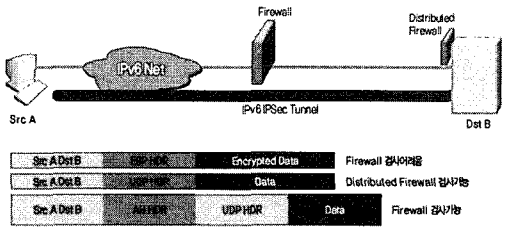
2.6 IPv6 주소 및 포트 정보를 이용한 접근제어

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.

IPSec터널링 사용 시에 발생하는 패킷 접근제어 취약성을 해결하기 위한 방안으로는 암호화된 패킷을 복호화할 수 있는 분산형 침입차단시스템의 사용과 AH만 적용한 암호화 패킷 사용을 들 수 있다. 그림 4와 같이 AH만 적용한 패킷은 침입차단시스템이 상위 계층의 정보를 기초로 패킷에 대한 접근제어를 하도록 한다.



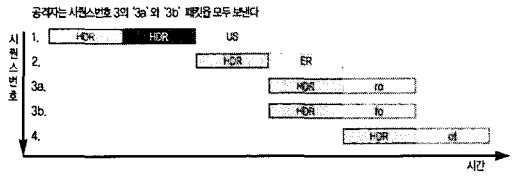
〔그림 4〕 침입차단시스템의 상위계층 정보 분석

2.7 전송 패킷의 단편화(Fragmentation)

IPv6에서는 단편화 과정이 IPv4와는 달리 단말 호스트에서만 이루어진다. 보안 위협은 공격자의 중복의 단편화된 패킷이 침입차단시스템에서 필터링 없이 목적지까지 전송하게 되면 목적지에서 패킷의 내용이 변경될 가능성이 있는 것이다.

그림 5는 공격자가 단편화 패킷의 일부 'fo'를 중복하여 보내는 예이다. 침입차단시스템이 중복된 단편화 패킷(3a, 3b)을 필터링하지 못한다면, 최종 목적지의

호스트는 분할된 패킷을 재조합(reassembly)할 때 중복된 단편화 패킷 중 어떤 패킷이 올바른 것인지 판단할 수 없게 된다. 이로 인해 시스템이 교착 상태나 충돌 문제가 발생하여 시스템 재시동과 같은 심각한 문제를 가질 수 있다. 이러한 위협의 대응 방안은 침입차단시스템이 단편화 패킷을 재조합하여 필터링을 적용할 수 있게 하는 것이다.



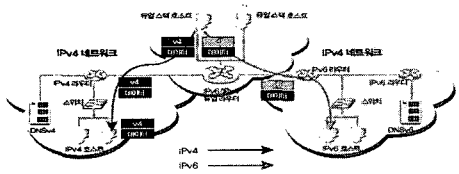
〔그림 5〕 단편화 패킷 중복 공격

Ⅲ. IPv4/IPv6 전환기술의 보안 위협과 대응 방안

현재, IPv4 망에서 IPv6 망으로의 전환(Transition)기술로는 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation)이 있다.

3.1 IPv4/IPv6 듀얼스택

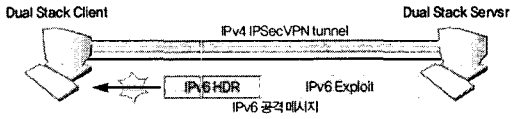
IPv6 단말이 IPv4 단말과 호환성을 유지하는 가장 쉬운 방법은 IPv4/IPv6 듀얼 스택을 제공하는 것이다. 그림 6은 듀얼 스택의 동작 개념도이다.



〔그림 6〕 듀얼스택의 동작 개념도

IPv4/IPv6 듀얼 스택 노드는 DHCP 등을 이용하여 해당 IPv4 주소를 얻고, 비상태형 자동 주소설정 기법 등을 이용하여 IPv6 주소를 획득할 수 있다. 따라서 듀얼 스택 노드의 DNS는 도메인 네임과 IP주소 간 매핑을 위해 IPv4와 IPv6 모두를 지원해야 한다.

듀얼스택 호스트에 대한 중요한 보안 고려사항은 IPv4에서 요구되는 보안수준이 IPv6 상에서도 동일하게 적용되어야 한다는 것이다. IPv4/IPv6 전환 시, 그림 7과 같이 듀얼스택 클라이언트가 IPv4에 대해서만 IPSec -VPN을 지원하고, IPv6에 대해서는 지원하지 않는다면 IPv6 패킷에 대한 안전한 통신을 보장하지 못한다.



〔그림 7〕 듀얼스택의 IPv4 터널링 지원

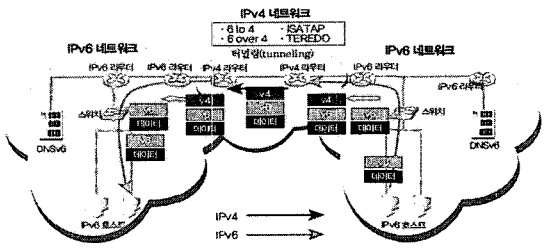
이러한 보안취약성에 대응하기 위해서 호스트 침입방지시스템(Host Intrusion Prevention), 개인용 침입차단시스템(Personal Firewall), VPN 클라이언트(VPN Client)와 같은 장비가 IPv4, IPv6 두 가지 프로토콜을 모두 인식하여 트래픽을 검사하고 차단할 수 있어야 한다. 예를 들어, IPv4에서 설정된 침입차단시스템의 ACL(Access Control List)은 IPv6의 ACL에도 반영되어야 한다. IPv6 네트워크는 IPv4 네트워크와 토폴로지가 달라서 ACL의 일관성을 유지하기 어렵지만 IPv4와 동일한 보안 수준을 유지하도록 해야 한다.

3.2 IPv4/IPv6 터널링

일반적으로 터널링은 네트워크를 보호하기 위해 설치된 침입차단시스템이나 침입탐지시스템을 우회할 수 있기 때문에 네트워크상에서 발생하는 보안 위협이다.

3.2.1 IPv6-in-IPv4 터널링

그림 8은 IPv6 데이터의 전송 경로에서 IPv4만을 인식하는 네트워크 구간에 대해 IPv6-in-IPv4 터널링을 적용한 예제이다.



〔그림 8〕 IPv6-in-IPv4 터널의 동작

만약, 침입차단시스템이 IPv4 구간 내에만 위치하는 경우, IPv4 환경에 맞추어 운영되는 대다수의 침입차단시스템은 IPv6 패킷의 내용을 인식하지 못하므

로 악의적인 IPv6 패킷을 차단할 수 없게 되는 보안 위협을 가지게 된다.

IPv6-in-IPv4 터널링을 이용하여 IPv4 침입차단 시스템을 우회하는 보안취약성을 해결하기 위해서는, 내부로 유입되는 IPv6 트래픽을 적절하게 검사하고 필터링할 수 있는 IPv6 기반의 침입차단시스템을 터널 종단에 설치해야 한다. 또한, 침입차단시스템은 IPv6에 대한 사이트 경계에서 IPv4에 사용된 ACL 규칙을 IPv6용으로 변환하여 반영해야 한다.

공격자가 ICMPv6 패킷을 이용하여 내부네트워크 호스트 주소에 대해 스푸핑 하는 것을 방지하기 위하여 내부로 유입되는 인그레스(ingress) 필터링 뿐만 아니라 외부로 유출하는 이그레스(egress) 필터링도 지원해야 한다.

IPv6-in-IPv4 터널 종단에서 디캡슐레이션된 IPv6 패킷은 글로벌 유니캐스트 주소를 가져야하므로 링크 로컬 주소를 갖는 패킷들은 침입차단시스템에서 폐기되어야 한다.

IPv6의 'path MTU discovery'기능은 패킷 단편화의 보안취약성에 대한 대응방안이지만, 이 기능이 모든 터널에서 구현되어 있지 않으므로 IPv6-in-IPv4로 캡슐화된 패킷의 최소 MTU값인 1280바이트로만 전송한다면 IPv4의 최대 path MTU값이 1500바이트 이므로 패킷 분할의 문제를 방지할 수 있다.

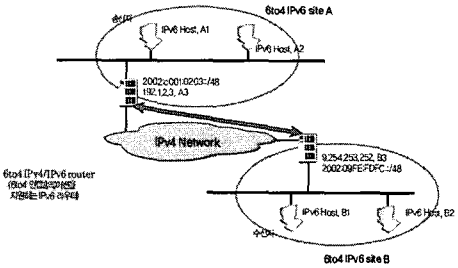
IPv6-in-IPv4 터널링 방법은 크게 수동 터널링(configured tunneling) 방식과 자동 터널링(automatic tunneling) 방식으로 구분된다. 일반적으로 관리자가 네트워크 구간의 모든 부분을 파악하여 네트워크를 안정적으로 운영할 수 있다는 측면에서 수동 터널링 방식이 보안상 더 안전하다.

3.2.2 6to4 터널링[9]

6to4 방식은 IPv6 주소에 IPv4 주소를 삽입하여 IPv4 망에서는 IPv4 패킷으로 라우팅 처리되고 IPv6 망에서는 IPv6 패킷으로 라우팅 처리되는 터널링 기술로 확장성이 뛰어나다(그림 9).

6to4에서 발생할 수 있는 주요한 보안위협은 다음과 같다.

- 터널링된 링크-로컬 패킷들이 6to4 가상 인터페이스를 원격 공격할 가능성이 있다. 만약 6to4 가상 인터페이스가 호스트의 다른 인터페이스로부터 분리되어 있지 않다면, 가상 인터페이스에 대한 원격공격은 모든 시스템에 영향을 미칠 수 있다.



〔그림 9〕 6to4의 동작

- 6to4 호스트들은 공격자가 조작한 IPv4 in IPv6 트래픽과 6to4 릴레이 서버로부터 수신한 트래픽을 구분하지 못한다. IPv6 노드에 대한 소스 주소 스푸핑과 DRDoS(Distributed Reflection of Denial-of-Service) 공격 모두에 취약하다.
- 공격자인 IPv6 노드가 자신의 실체를 숨기는 수단으로써 릴레이 서버를 이용할 수 있다. 즉, 공격자는 터널링된 패킷을 스푸핑하여 IPv4 호스트를 공격할 수 있다.
- 6to4 릴레이 서버는 로컬 망에 대한 브로드캐스트 공격(broadcast attack)에 사용될 수 있다.

대응 방안으로 가상 인터페이스에 대한 위협은 ACL을 사용하여 대응할 수 있으며 관리자는 서로 다른 6to4 주소 간에는 릴레이하지 않도록 6to4 릴레이 서버를 설정해야 한다. 브로드캐스트 공격은 6to4 주소와 유사한 브로드캐스트 주소를 목적지 주소로 갖는 패킷에 대해 필터링하는 ACL을 설정하여 대응할 수 있다. 일반적으로 6to4 릴레이는 6to4 주소를 검증하여 보호할 수 있다. 즉, 6to4 주소내의 IPv4 주소가 글로벌 유니캐스트 주소이고, 실제 사용되는 주소인지를 검증해야 한다.

3.2.3 ISATAP(Intra Site Automatic Tunnel Address Protocol) 터널링

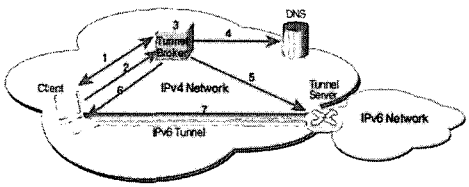
ISATAP는 IPv4 네트워크 내부에 존재하는 듀얼스택 호스트가 IPv6 호스트와 통신을 하기위한 방법으로 IPv4 터널링을 위한 별도의 라우터가 필요하다.

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.

3.2.4 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.



〔그림 10〕 터널브로커의 동작

그림 10의 동작 과정은 다음과 같다.

(1)먼저 클라이언트와 터널 브로커 사이에 AAA를 통한 인증을 수행한다.

(2)클라이언트가 터널 브로커에게 터널 정보를 요청한다.

(3)터널 브로커가 터널 서버, IPv6주소, 터널 유지 시간 등을 선택한다.

(4)터널 브로커가 DNS에 클라이언트의 IPv6주소를 등록한다.

(5)터널 브로커는 터널 설정 정보를 터널 서버에 전달한다.

(6)터널 브로커가 클라이언트에게 터널 파라미터, DNS 명을 전달한다.

(7)설정 정보를 통하여 클라이언트와 터널 서버 간에 터널링을 생성한다.

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. 인증의 방법에는 아이디-패스워드 기반의 간단한 방법부터 KDC(Key Distribution Center) 등을 이용한 방법이 가능하다. RFC3129[2] 에서는 사용자에게 Kerberos[3] 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. 예를 들어, A네트워크에서 터널을 경유하여 B네트워크로 전송되는 패킷의 목적지 주소가 A네트워크에서만 유효하다면 B네트워크에서는 필터링이 돼야 한다. 또 다른 대응 방안은 터널의 상태를 파악할 수 있는 모니터링 프로그램을 운영하여 악의적인 패킷을 대량으로 전송하는 공격을 탐지 및 차단하여 대응할 수 있다.

3.2.5 DSTM(Dual Stack Transition Mechanism) 터널링[10]

DSTM의 기능은 듀얼스택 호스트 상의 IPv4응용이 IPv4호스트와 통신을 필요로 하는 환경에서 IPv4-in -IPv6터널링을 제공하는 것이다. DSTM 터널링을 구성하기 위해서는 표 2과 같은 세 가지 종류의 장비가 필요하다.

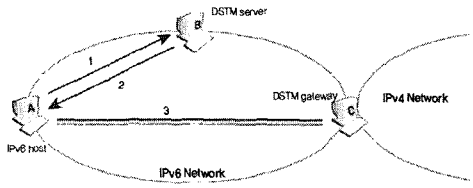
〔표 2〕 DSTM 터널링을 위한 구성요소

종류	장비	동작
A	IPv4/IPv6 듀얼스택 호스트	IPv6-only 네트워크 내부에 존재하지만 IPv4를 이용해 통신하기를 원함
B	DSTM 서버	IPv4 address pool을 유지하고 필요시 할당함
C	DSTM 게이트웨이 (또는 TEP,Tunnel End-Point)	IPv6 패킷에 IPv4캡슐화(encapsulation) 및 비캡슐화(decapsulation)를 수행

2) Requirements for Kerberized Internet Negotiation of Keys

3) 네트워크 사용자를 인증하는 것과 관련하여 미국 MIT의 아테네 프로젝트에서 개발된 네트워크 인증 표준

DSTM 터널링 동작은 그림 11과 같다. 1, 2번 과정은 A가 B에게 임시 IPv4 주소를 요청하여 응답을 받는 과정으로 DHCPv6나 RPC를 통해 이루어질 수 있다. 응답 메시지에는 임시 IPv4 주소뿐만 아니라 해당 주소의 유효기간과 DSTM 게이트웨이 정보가 포함된다. A는 IPv4 프로토콜 스택을 설정하여 IPv4 네트워크로 향하는 IPv4 패킷을 IPv6 주소로 캡슐화하여 C까지 전송한다. C는 디캡슐화를 수행하기 위한 IPv4/IPv6 주소 맵핑 테이블을 유지한다.



(그림 11) DSTM 동작

DSTM에서는 공격자가 다른 호스트의 세션을 가로챌 수 있는 보안위협이 있다. 예를 들어 그림 11의 A가 IPv4주소를 할당받아 IPv6 터널을 통해 IPv4 네트워크와 통신하는 경우를 생각해보자. 만약, 공격자가 A의 IPv4 소스 주소를 도용하여 IPv4-in-IPv6 패킷을 보낸다면, C와 A 사이의 터널은 끊어지고, C와 공격자 사이의 터널로 교체된다.

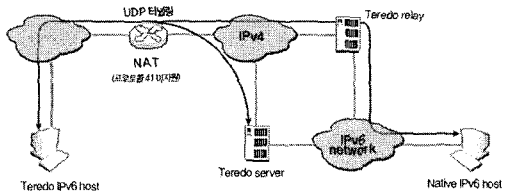
대응방안으로 DSTM 서비스가 제공하는 인증기능이 미비하므로 관리자는 별도의 인증 메커니즘을 구축·운영하여야 한다. 특히, DSTM 서버에서는 임시 IPv4 주소를 요구하는 호스트들에 대한 인증이 필요하다. 또한, 관리자는 현재 사용 중인 터널이 DSTM 서버에 의해 정상적으로 생성된 것인지를 항상 확인하고 비정상적인 트래픽을 차단하여야 한다.

3.2.6 Teredo 터널링

Teredo 터널링은 IPv6-in-IPv4 터널링 패킷을 지원하지 않는 IPv4용 NAT가 운용되는 환경에서 듀얼스택 노드에 UDP 상의 터널링 패킷을 통하여 IPv6 통신을 제공하는 기술이다.

그림 12는 Teredo IPv6 호스트가 UDP 터널링을 이용하여 Teredo 서버에게 터널링에 대한 요청을 보내고 Teredo 릴레이를 통한 native IPv6 호스트와의 통신 과정을 보여주고 있다.

NAT에서 Teredo관련 서비스를 허용시키고 침입차단시스템에서도 패킷 필터링을 허용시키는 경우에 공격자가 허용된 서비스들을 이용한 공격이 가능하다. 이러한 환경에서 공격자는 RS를 가로채거나 스푸핑된 RA를 전송하거나 Teredo 클라이언트에게 잘못된 주소를 제공하게 할 수 있다. 이러한 동작으로 클라이언트들의 통신에 대한 릴레이기능을 이용하여 중간자 공격 및 Teredo서버를 이용한 반사공격이 가능하다.



(그림 12) Teredo 동작

NAT상에 생성된 보안 취약성은 필요한 서비스에 대해서만 NAT에서 허용하고 IPv6용 개인 침입 차단 시스템 및 IKE, AH, ESP 같은 IPv6 보안 서비스를 사용하여 대응할 수 있다. 중간자 공격에 대한 대응방안으로는 클라이언트들이 외부로 IPv6패킷을 전송하는 경우, IPSec을 이용하여 무결성 및 기밀성을 제공하게 하는 것이다.

3.3 IPv4/IPv6 변환기술

IPv4/IPv6 변환은 네트워크/전송/응용 계층에서 수행될 수 있고, 통신 호스트 간 트래픽 변환과 중계를 제공하는 서버를 필요로 하며, 변환을 수행하는 계층이 상위일수록 성능이 저하되는 특징을 갖는다. 본 절에서는 네트워크 계층에서의 변환기술에 대한 보안 위협 및 대응 방안만을 기술한다.

3.3.1 NAT-PT/NAPT-PT (Network Address Translation-Protocol Translation /Network Address Port Translation-Protocol Translation)

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 포트 번호를 통하여 구분하는 기능을 갖는다.

IPv6 호스트 A가 IPv4 호스트 B로 패킷을 송신할 때, 그 패킷은 IPv6 주소를 가지므로, IPv4로 변환해야 한다. 이때, IPv6에서 생성된 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 중단된 경우, 공격자가 IPv6 호스트에 조작된 IPv6 프리픽스를 할당하여, IPv4 호스트로 전달될 모든 패킷을 가로챌 수 있다. 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 수행하는 것이다. 즉 공격자가 소스 주소를 위조하지 못하게 하고, 동일한 도메인에 있는 다른 노드에 반사공격을 수행하지 못하게 한다. IPv4 주소고갈 공격(Address Depletion Attack)은 IPv6 노드의 TCP/UDP 포트를 IPv4 노드의 주소에 부합하는 TCP/UDP 포트로 매핑을 지원하는 NAT-PT를 사용하여 방지할 수 있다. NAT-PT 게이트웨이는 필터링을 통해 IPv4 소스 주소가 브로드캐스트/멀티캐스트 주소인 모든 패킷들을 폐기함으로써 서비스거부공격을 방지할 수 있다.

Ⅳ. 결 론

IPv6는 IPv4에 비해 향상된 보안기능을 제공하고 있으며, IPsec의 기능을 최대한으로 활용하는 경우, 많은 보안공격을 예방할 수 있다. 다만, IPv6에서의 보안이슈는 IPv4에서와 같이 공격자가 악의적인 의도를 갖고 메시지 변조, 위장 등 비정상적인 행위를 통한 공격에 노출되어 있으며, 이를 해결하기 위해서는 자체 IPsec 및 필터링 기능 등을 최대한 활용하고, Firewall, IDS 등의 부가적인 보안장비를 활용하여 예방할 필요가 있다. 또한 응용계층에서의 보안문제는 IPv6 네트워크 계층에서 모두 해결할 수 없으므로 계층별 보안 솔루션을 이용하여 사전에 예방하는 것이 중요하다.

현재, 제품별로 IPsec 기능이 제한적으로 지원되는 경우가 많으며, 향후 IPsec 키관리 등 표준화에 대한 진전과 함께 IPsec 서비스가 점차 안정적으로 제공될 것으로 예상된다.

또한 전국적인 규모의 IPv6 네트워크 구축이 완료되기까지 IPv4와 IPv6가 혼재되어 공존할 것으로 예상됨에 따라, IPv4/IPv6 전환기술에 대한 보안취약성을 분석하고 관련 보안 기술 및 보안대책을 수립해야 한다.

따라서, 안전한 IPv6 운영을 위한 IPv6 보안위협 분석 및 보안대책을 마련하고, 공격자의 위장, 메시지 변조, 오남용에 대한 적절한 대응 기술 개발이 필요하다.

참 고 문 헌

[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] "SEC-2003: IPv6 Security Threats," http://www.cisco.com/

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

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

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

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

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

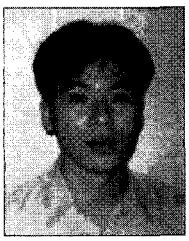
[11] "Review of IPv6 Transition Scenarios for European Academic Networks," IPv6 Conference, 2002

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

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

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

〈著 者 紹 介〉



신 동 명 (Dong-Myung Shin)

2000년 2월 : 대전대학교 컴퓨터공학과 공학석사
2003년 8월 : 대전대학교 컴퓨터공학과 공학박사
2001년 7월 ~ 현재 : 한국정보보호진흥원 정보보호기술단 선임연구원
〈관심분야〉 멀티캐스트 보안, 소프트웨어 보안 취약성 분석, IPv6 보안 등

현 호 재 (Ho-Jae Hyun)

1999년 2월 : 건국대학교 컴퓨터공학과 공학석사
2005년 8월: 건국대학교 컴퓨터공학과 공학박사
2005년 2월 ~ 현재 : 한국정보보호진흥원 정보보호기술단 위촉연구원
〈관심분야〉 멀티캐스트 보안, IPv6 보안, 홈 네트워크 미들웨어, QoS 등

윤 미 연 (Mi-youn Yoon)

2002년 2월 : 숭실대학교 컴퓨터학과 공학석사
2005년 8월 : 숭실대학교 컴퓨터학과 공학박사
2005년 6월 ~ 현재 : 한국정보보호진흥원 정보보호기술단 선임연구원
〈관심분야〉 IPv6 보안, 멀티캐스트 보안, 센서네트워크 보안

원 유 재 (Yoo-yae Won)

1987년 : 충남대학교 전산학과 공학석사
1998년 : 충남대학교 전산학과 공학박사
1987년 ~ 2001년 : 한국전자통신연구원 팀장
2001년 ~ 2004년 : 안랩유비웨어 연구소장
2004년 ~ 현재 : 한국정보보호진흥원 정보보호기술단 팀장
〈관심분야〉 IPv6 보안, 멀티캐스트 보안, 무선 인터넷 보안, PKI 등