특집

IPv4/IPv6 연동환경에서의 차세대 보안 기술

신명기(한국전자통신연구원)

요 약

본 고에서는 IPv4/IPv6 연동 환경에서 고려해야 할 차세대 보안 기술들에 대해 기술한다. IPv6는 국내외로 2008년부터 본격적으로 도입되기 시작하여 2010년에는 상용망 구축이 활발해 질것으로 예상되며, 기존 IPv4와의 연동에 대한 요구는 2020년까지는 지속적으로 유지될것으로 보인다. 이때 반드시 연구가 선행되어야 할 것 중의 하나는 보안 문제로 현재 표준화 관점과 망 운영 관점에서 분석하고 이를 해결하기 위한 연구가 진행중이다. 본 고에서는 이를 IPv6 프로토콜 보안 문제와 IPv4/IPv6 연동 보안 문제로 나누어 분석하고, 실제 방화벽 등에서 이러한 보안 문제를 해결하기 위한 방법 등을 기술한다.

I. 서 론

IPv6(Internet Protocol version 6)는 인터넷 국제표준화 기구인 IETF(Internet Engineering Task Force) IPv6 워킹그룹에서 1988년부터 표준화 작업을 시작한 차세대 IP 프로토콜로서, 현재 사용되고 있는 IP 프로토콜인 IPv4를 대신하여 2008년 경부터 WiBro, 홈 네트워크, 센서 네트웍 등 신규 인터넷 연결 망을 중심으로 도입될 예정이다. IPv6 도입시 중요하게 고려되어야 할 사항중에 하나는 기존 IPv4 망과의 연동(Interworking) 문제로 기존 IPv4 단말이 완전히 소멸될 것으로 예상되는 2020년 정도까지는 기존 IPv4 망과 IPv6 망이 공존할 것으로 예측되고 있다. 이를 위해 IETF에서는 NGTrans(Next Generation Transition), V6ops(IPv6 Operations) 워킹그룹을 별도로 두어 IPv4/IPv6 연동을 위한 다양한 전환 메커니즘(transition mechanism)을 개발중에 있다. [표 1]은 현재 개발 완료되었거나 개발중인IPv4/IPv6 전환 메커니즘의 종류 및 적용환경을 나타낸다[1-6].

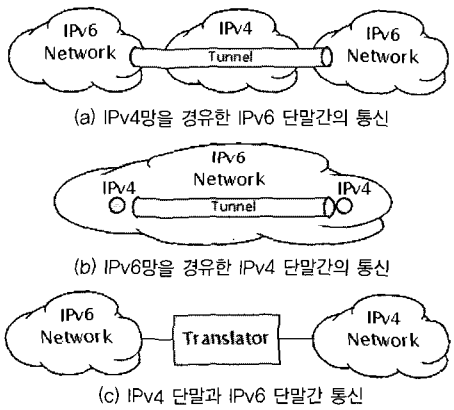
현재 개발된 IPv4/IPv6 전환 메커니즘에서의 중요한 고려사항 중 하나는 보안 문제에 있다. 또한 IP 프로토콜이 처음 개발되어 제안된 1970년 이후, IP 보안에 대한 문제는 끊임없이 지속적으로 연구되어 왔으며, 현재도 인터넷의 가장 취약한 문제점 중의 하나로 보안 문제를 꼽고 있을 정도로 많은 연구와 관심이 진행되고 있는 분야중의 하나이다. IPv6 차세대 인터넷 프로토콜은 이러한 IP의 문제점을 보다 개선하기 위해

〈표 1〉 적용환경 별 IPv4/IPv6 전환 메커니즘

적용환경		전환 메커니즘	표준문서
IPv4 망을 경유한 IPv6 단말간의 통신 (IPv6-over-IPv4)	사이트 내 (Intra-site)	설정 터널 (Configured Tunneling)	RFC4213 [1]
		6to4	RFC3056 [2]
	사이트 간 (Inter-site)	ISATAP	RFC4124 [3]
	NAT Traversal 지원	Teredo	RFC 4380 [4]
IPv4 망을 경유한 IPv6 단말간의 통신 (IPv4-over-IPv6)		DSTM	I-D(초안) [5]
IPv4 단말과 IPv6 단말간 통신 환경 (IPv6-to-IPv4 또는 IPv4-to-IPv6)		NAT-PT	RFC2766 [6]
		DSTM	I-D(초안) [6]

IPsec의 구현을 기본(mandatory)으로 하는 등 보다 안전한 인터넷(Secure Internet)을 구축하기 위한 설계 철학을 담기도 하였다. 그러나, 최근 IETF 내의 보안 그룹 등에서 IPv6 프로토콜에서의 확장 헤더의 사용, IPv4/IPv6 전환 메커니즘의 사용시 보안 문제가 발생할 수 있다고 연구결과를 발표하고, 이에 대한 보안 확인을 반드시 하도록 권고하고 있다[7-8].

본 고에서는 IPv6 도입에 따른 보안 위협 요소를 크게 두가지로 구분하여 분석한다. 첫째는 IPv6 프로토콜 자체에 대한 문제로 처음 설계 당시 기존 IPv4와는 다른 확장된 프로토콜을 설계하고자 추가했던 기능들이, 보안 관점에선 문제가 되는 것으로 보고되고 있다. 물론 이러한 문제점들은 IPv6의 궁극적인 문제들은 아니며, 기존 IPv4 프로토콜 역시, 해커들의 공격과 이에 대한 보안 문제의 해결 이라는 반복을 통해 보다 안전한 프로토콜로 발전해 나갔던것 처럼, IPv6 역시, 이러한 보안 문제점들도 IPv6 프로토콜의 보안기능 수정과, 방화벽, 침입방지시스템(IPS, Intrusion Prevention System)에서의 관련 기능 추가 등으로 인해 해결될 수 있을 것으로 생각된다[9]. 두 번째 문제로는 IPv4/IPv6 연동 환경에 따른 보안 문제들로서, 실제 IPv4 프로토콜, 혹은 IPv6 프로토콜 자체로는 문제가 없지만, 두 망이 혼재되는 상황에선 예상치 못했던 보안 위협 문제가 발생할 수 있다. 본 고에서는 이러한 두가지 관점에서 IPv6 전환시 발생할 수 있는 보안 문제점들을 기술한다.



〈그림 1〉 IPv4/IPv6 전환 메커니즘 적용 환경

〈표 1〉 IPv6 프로토콜 보안 위협 요소

IPv6 프로토콜 보안 위협 요소	보안 관련 문제점
확장 헤더	라우팅 헤더, 홉-바이-홉, 목적지 옵션, 프레그먼트 확장 헤더를 이용한 DoS 공격
다양한 주소 처리	방화벽/IPS에서의 링크-로컬(link-local), 유니크 로컬 (unique-local), 글로벌(global) 등 주소별 의미적 필터링 미정의
ICMPv6 / ND	RA/RS, NA/NS 메시지들의 안전한 전송 필요, 주소 보안 확장 방법을 이용한 DDoS 공격
멀티캐스트/애니캐스트	멀티캐스트 패킷 오류에 대한 응답 메시지 범람 및 애니캐스트 의미적 필터링 미정의
IPsec 사용	글로벌 점대점 IPsec 사용을 위한 PKI, 키교환 방법 미정의
MIPv6	방화벽/IPS 에서의 BU, RR 패킷 차단

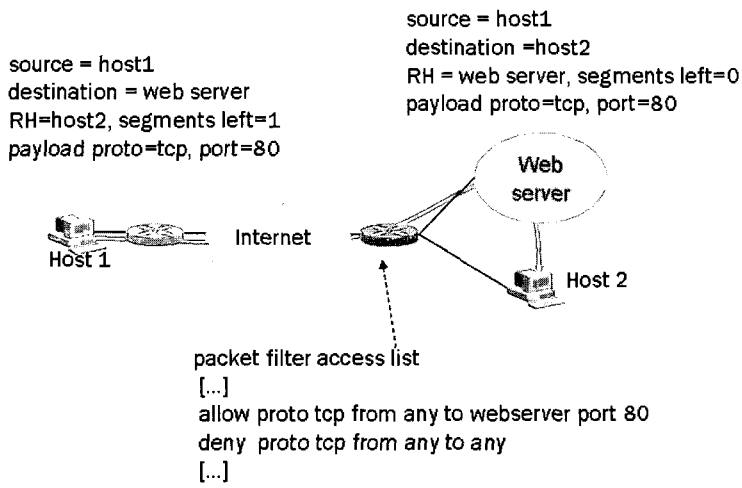
II. IPv6 전환 환경에서의 보안 요소 분석

1. IPv6 프로토콜 보안 위협 요소

IPv6 프로토콜 자체에 대한 보안 위협 요소들은 [표 2]와 같이 정리된다. II 장에서는 각각의 보안 위협요소들에 대한 분석과 이를 해결하기 위한 방화벽/IPS 등에서의 지원 방안 등을 기술한다[13].

가. 확장 헤더

IPv6는 처음 설계 당시 보다 다양한 프로토콜의 설계 및 확장성을 용이하게 하기 위해 라우팅 (Routing), 홉-바이-홉 (Hop-by-Hop), 목적지 (Destination Option) 등 기존 IPv4에는 없는 새로운 확장 헤더 등을 추가하였으며, 기존 IPv4에 옵션으로 정의되어 있는 프래그먼트 헤더 등도 새로이 IPv6의 확장 헤더로 정의하여 사용한다. 이 경우, 보안 관점에서의 문제점은 이러한 확장 헤더들이 기존 단말들에서 패킷의 포워딩, 패킷 재조합 등의 새로운 동작들을 가능하도록 할 수 있다는 데 있다. 이러한 경우, 확장 헤더가 잘못 사용되거나, 공격을 받으면, 심각한 보안 위협 요소로 동작할 수 있다. 라우팅 헤더의 경우, 라우팅 헤더 내에 열거된 주소 목록에 따라 소스 라우팅 하는 기능을 가지고 있으며, 따라서 [그림 2]와 같이 host1내에 라우팅 헤더 내에 host2에 대한 주소를 포함하여 패킷을 전달하게 되면, 내부을 보호하는 패킷 필터링 규칙이 [그림 2]와 같이 설정되었더라도, 이 패킷을 필터링 할 수 없으며, 이 패킷을 받은 웹 서버는 라우팅 헤더의 규칙에 따라 이 패킷을 host2로 포워딩 하게 되어, host2로의 공격을 막을 수 없게 된다. 따라서 내부 망을 보호하는 패킷 필터링 규칙에는 기존 헤더에 대한 수신자, 송신자 주소 및 포트에 대한 검사 외에도 확장 헤더들에 대한 정확한 필터링 규칙들이 설정 가능하도록 확장 되어야 한다. 그렇지 않으면 앞선 라우팅 헤더의 오용 예에서 보듯이 DoS (Denial of Service) 공격들을 받을 수 있다. 이밖에도 라우팅 헤더, 홉-바이-



〈그림 2〉 라우팅 헤더의 오용 예

홉, 목적지 헤더들이 사용되면, 미들박스에서의 확장 헤더의 처리 여부, 확장 헤더의 체인 처리 규칙, 미정의된 확장 헤더의 처리 규칙, 과도하게 사용된 홉-바이-홉 옵션과 라우터 얼러트 (Router Alert) 옵션 등의 처리도 고려되어야 한다. 또한 프레그먼트 헤더의 경우에도 DoS 공격이 가능하며, 예를들어, 방화벽/IPS 등에서는 프레그먼트 헤더가 포함된 패킷은 검사하여 마지막 프레그먼트 된 부분을 제외하고, 1280 옥텟 이하의 프레그먼트 부분이 포함된 패킷들은 DoS 공격 패킷일 가능성이 많음으로 폐기하여야 한다.

나. 다양한 주소 처리

IPv6의 장점중의 하나는 많은 양의 주소를 제공할 수 있고, 이를 링크-로컬(link-local), 유니크 로컬 (unique-local), 글로벌(global) 주소 등으로 분리하여 다양하게 사용할 수 있다는 점이다. 그러나 이러한 다양한 주소 방식은 사용은 보안 관점에서는 또 다른 문제점을 가지고 있다. 이러한 다양한 주소 사용에 대한 각 주소의 정확한 의미 (semantics) 들을 방화벽/IPS 등에서 이해하고 처리하여야 하기 때문이다. 또한 IPv6 주소 구성은 전체 128 비트 주소체계에서 64 비트의 인터페이스 ID (IID) 를 사용하는 구조를 가지고 있으며, 망 구성의 가장 기본적인 단위인 서브넷은 /64로 정해져 있다. 이 경우, 한 서브넷 내에 모두 2^{64}개만큼의 단말 수를 가질 수 있게 되어, 기존 IPv4에서 사용되던, ping 탐색이나, 포트 스캐닝과 같은 공격 및 보안 방법 등을 사용할 수 없게 된다.

다. ICMPv6 / 이웃탐색 기능 (ND, Neighbor Discovery)

IPv6의 또다른 장점중의 하나는 기존 ICMP 기능에 다양한 기능을 추가한 ICMPv6와 ND 기능을 들 수 있다. IPv6는 이러한 제어 메시지들을 이용하여 주소 자동설정(auto-configuration) 이나 라우터 발견(router discovery), 망 재설정 (network renumbering) 과 같은 보다 자동화된 기능들을 구현한다. 보안 관점에서의 이러한 제어 메시지들의 문제점은 이러한 메시지들이 오

용되어 사용되면, 전체 자동화 관점에 큰 문제점을 야기시킬 수 있다는 데 있다. 예를 들어 주소 자동설정에 사용되는 RA(Router Advertisement) 메시지가 인증받은 라우터로부터 받지 않고, 공격자에 의해 전송되는 RA 메시지를 받아, 주소를 설정하기 되면, 단말에서는 잘못된 주소로 설정이 되는 문제가 발생할 수 있다. 또한 IPv6에서 주소 설정시 추가로 사용가능한 주소 보안 확장 방법 (Address Privacy Extension) 역시, 잘못 사용되면, DDoS (Distributed DoS) 공격 처럼 보일 수 있어, 이에 대한 사용시에는 주의를 기울여야 한다[10].

라. 멀티캐스트/애니캐스트

IPv6에서는 기존 IPv4 보다는 다양한 멀티캐스트, 새롭게 정의된 애니캐스트 방식을 제공한다. 멀티캐스트에서의 보안문제는 기존 유니캐스트 경우보다, 더욱 심각할 있다. 그 이유는 멀티캐스트 패킷의 특성상, 다수의 많은 가입자들에게 잘못된 패킷이 범람(flooding) 될 수 있기 때문이다. 현재 ICMPv6에서는 멀티캐스트 패킷이 잘못 전달되었을 경우에는 이에 대한 오류 응답 메시지를 보낼 수 있도록 허용하고 있어, 이에 대한 오류 메시지가 잘못 사용될 경우, 망 전체를 오류 메시지로 범람시킬 수 있다. 또한 애니캐스트의 경우는 정당한 패킷의 식별과 이에 따른 보안 방법도 새롭게 강구되어야 한다. 애니캐스트 방식은 기존 IPv4 에는 없는 새로운 주소 유형 및 서비스 방법이기 때문이다. 이러한 멀티캐스트/애니캐스트 보안 문제 해결을 위해서는 기존 방화벽/IPS 등에 이를 위한 새로운 필터링 규칙등이 정의되어야 한다.

마. IPsec

기존 IPv4에서의 IPsec은 주로 VPN 과 같은 안전한 원격 제어 서비스 용으로만 주로 이용되어 왔으나, IPv6의 경우는 앞선 설명한 대로 모든 글로벌 인터넷 망 상의 통신 시 IPsec의 사용이 가능하게 되어, 보다 안전한 IP 통신망을 구축할 수 있을 것으로 기대된다. 하지만, 실제 사용 및 적용면에서도 보면, 아직 전역적으로 사용가능한 PKI 및 키 교환 방법 등에 대한 실현 가능성에 의구심을 가지고 있으며, IPsec과 이동성 지원 방법들은 아직 통합되지 않은 상태이다. 글로벌 인터넷 상의 점대점(end-to-end) 관점에서의 IPsec에 대한 실제 사용 측면에서의 이러한 문제점들은 아직 풀어야 할 숙제로 남아 있다.

바. MIPv6 (Mobile IPv6)

IPv6 프로토콜 자체에 대한 마지막 보안 고려사항으로는 이동성 지원을 제공하는 MIPv6의 보안 문제점들을 들 수 있다. IPv6 장점중의 하나는 MIPv6 기능의 기본으로 탑재되어 모든 단말들이 자유롭게 이동하면서 IP 연결성을 유지할 수 있다는 데 있다. 이를 위해 단말과 홈 에이전트(HA, Home Agent) 등 간에는 MIPv6라는 프로토콜을 사용하여 기존 MIPv4와는 달리 경로 최적화(route optimization) 기능 등을 제공할 수 있다. 그러나 이러한 기능을 제공하기 위해서는 이동단말과 HA 사이에 인증과 동적인 바인딩 수정(Binding Update) 과정이 요구되며 이를 위해선 이동단말과 HA 사이에 안전한 통신이 선행되어야 한다. 이를 위해 이동단말과 HA 사이에는 필요한 BU(Binding Update) 패킷들을 반드시 IPsec ESP 통신을 이용하도록 하고 있다. 이 경우, 현재 나와있는 대부분의 방화벽들은 이러한 BU, RR(Return Routability) 패킷들을 정

상적으로 통과시키지 못한다는 점이며, 이를 해결하기 위해서는 방화벽/IPS 등에서 MIPv6 제어 메시지들을 인식 할 수 있도록 추가 개발이 이루어져야 한다.

2. IPv4/IPv6 연동환경 보안 위협 요소

IPv6가 도입되어 기존 IPv4 망과 새롭게 구성된 IPv6 망이 공존하게 되면, 보안 관점에서는 기존 IPv4와 IPv6 에는 없던 새로운 문제점들이 야기될 수 있다. 이러한 문제점들은 IPv4/IPv6가 공존되는 기간동안에 발생될 것이며, IPv6 가 완전히 도입이 완료되고, IPv4가 사라지게 되면, 더 이상 이러한 문제는 없을것으로 보인다. 그러나 앞서 설명한 다양한 IPv4/IPv6 전환 메커니즘들이 망 상에서 존재하고 동작하는 한, IPv4/IPv6 연동 환경에서의 보안 문제점들이 계속 문제화 될 것으로 보인다. IPv4/IPv6 연동환경에서의 보안 위협 요소들은 크게 터널링의 사용, IPv4 주소내장 IPv6 주소 사용 및 IPv4/IPv6 전환 메커니즘의 사용 등의 구분하여 분석할 수 있으며, 본 고에서는 IPv4/IPv6 전환 메커니즘 중에서 대표적으로 사용될 6to4[2]와 NAT-PT[6]를 중심으로 기술한다.

가. 터널링 (Tunneling)

6to4[2], ISATAP[3] , DSTM[5], Teredo[4] 등 대부분의 IPv4/IPv6 전환 메커니즘들은 IP-in-IP 터널링 방법을 사용한다. 이러한 터널링 방법에서의 보안 문제점 들로는 망 토폴로지를 더욱 복잡하게 하여 인그레스 필터링과 같은 토폴로지-기반 보안 문제들을 야기시킬 수 있다는 데 있다. 인터넷 망에서는 연결하고자 하는 상대 단말의 유형이나 서비스 등에 대해 미리 확인할 수 없는 것이 일반적이다. 따라서 복잡한 터널링 구조를 갖는 IPv4/IPv6 공존 망에서는 상대에 대한 프로토콜 버전과 망 구조를 더욱 복잡하게 하여 상대 노드에 대한 인증 등 미리 확인이 필요할 시에는 보안 관점의 문제들이 발생할 수 있다. 또한 IP-in-IP 패킷 상에서의 송신자 및 수신자 주소 등이 스푸핑(spoofing)되면, 또다른 보안 문제를 야기 시킬 수 있으며, 이를 위한 터널링 방법에 IPsec을 기법을 추가하여 이에 대한 문제를 해결하려는 작업이 진행중이다.

나. IPv4 주소내장 IPv6 주소 (IPv4 address embedded IPv6 address)

터널링과 함께 IPv4/IPv6 전환 메커니즘들이 사용하는 대표적인 기법중에 하나는 128 비트를 갖는 IPv6 주소 체계내에 32비트의 IPv4 주소 체계를 포함시키도록 하는 방법이다. 대표적으로 6to4[2], NAT-PT[6], ISATAP[3] 등이 이러한 방식을 사용한다. 이러한 주소 방식을 사용하면, 기존 IPv6 단말에서 IPv4 단말 주소를 쉽게 얻어낼 수 있다는 장점을 가지고 있으나, 이러한 주소의 구성은 보안 관점에서의 새로운 문제점들을 야기 시킬 수 있다. 예를들어 6to4 주소로 "2002:0a03:000c::7f00:0002"는 IPv6 주소관점에서 보면 아무런 문제가 없는 주소이나, 실제 6to4 주소체계에서 "2002" 이하의 32비트를 나타내는 "0a03:002c:"는 IPv4 주소가 내장되어 있는 것으로 10진수로 "10.3.0.12"를 나타내어 IPv4의 사설주소(private address)가 된다. 6to4에서 내장되는 IPv4 주소는 반드시 공중 주소(public address) 만을 사용하도록 되어 있어, 보안 관점에서 "2002:0a03:000c::7f00:0002"는 잘못된 공격일 가능성이 많음으로 방화벽 등에서 폐기하여야 한다. 따라서 주소 관점에서 보면, 기존 IPv4

주소 필터링, IPv6 주소 필터링 규칙 외에도 IPv4/IPv6 전환 메커니즘이 사용되게 되면, { Pv4의 오용된 주소형태} × {IPv4 주소내장 IPv6 주소형태} 등을 모두 검사해야 한다.

다. 6to4

6to4[2] 메커니즘은 동적 터널링을 사용하는 대표적인 IPv4/IPv6 전환 메커니즘 중의 하나이다. 6to4에서의 보안 문제점은 6to4 라우터가 어떠한 릴레이가 보안상 합법적인지 확인이 불가능하며, 잘못 혹은 부분적으로 구현된 6to4 라우터나 릴레이 등은 보안상의 검사가 반드시 요구되며, 실제 DoS 공격등이 6to4 구조하에 발생하면, 그 문제가 발생할 곳이 추적하기가 어렵고, 마지막으로 6to4 릴레이가 사용되면, 다른 릴레이 기능과 마찬가지로 보안상 오용될 가능성이 많다는 점이다[11]. 이러한 여러 가지 문제들로 인해 6to4 메커니즘은 많은 기능상의 장점에도 불구하고 현재 도입이 늦어지고 있으며, 일반적인 망의 전환 메커니즘으로는 사용되지 않은 가능성이 높다.

라. NAT-PT

NAT-PT(Network Address Translation - Protocol Translation)[6]는 IPv4 전용단말이 IPv6 전용단말과 통신할 수 있는 대표적인 메커니즘이다. NAT-PT의 단점으로는 IPsec 및 보안 키 관리가 어렵고, DNSSEC이 적용 불가능하며, NAT-PT 박스에 대한 주소 풀 자원을 고갈시키는 DoS 공격들을 방지하기 어려운데 있다. 이러한 보안상의 문제들로 인해 NAT-PT 역시 일반적인 솔루션보다는 홈 네트웍, 3GPP와 같은 특정 망에 한정되어 사용될 가능성이 많다. 최근 NAT-PT의 보안 문제와 관련해서는 NAT-PT에서도 IPsec의 사용이 가능하도록 IPsec Traveral 기능을 추가 개발하는 연구가 진행중이다.

III. IPv4/IPv6 연동환경에서의 안전한 보안 규칙 요약

II, III 장에서 분석한 보안 위협 요소들을 해결하기 위해 방화벽, IPS, 보안 관련 장비 등에서 추가 고려, 정의해야 할 필터링 규칙들을 요약하면 다음과 같다[12].

- ▷ 방화벽에서는 어떠한 확장 헤더 등이 통과하고 처리해야 하는 지를 정의
- ▷ 보더 라우터에서는 내부 망에서 사용될 IPv6 주소 필터링 규칙 정의
- ▷ ICMPv4 패킷 규칙에 아래와 같은 ICMPv6 필터링 규칙 추가
  ICMPv6 Type 2 - Packet too big
  ICMPv6 Type 4 - Parameter problem
  ICMPv6 Type 130-132 - Multicast listener
  ICMPv6 Type 133/134 - RS and RA
  ICMPv6 Type 135/136 - NS and NA
- ▷ 1280 옥텟 이하의 모든 프레그먼트 부분은 폐기 (마지막 프레그먼트 부분은 제외)
- ▷ IPv6 지원 인그레스 필터링 (Ingress filtering) 정의
- ▷ 터널링 및 IPv4/IPv6 전환 메커니즘에 사용되는 프로토콜 및 포트번호 정의
  IP protocol 번호 41 (IP-in-IP 터널 용), UDP 포트 3544 (Teredo 용) 통과
- ▷ 보안 강화가 필요한 중요한 시스템의 경우는 static ND 엔트리 정의
- ▷ BGP, IS-IS 등 라우팅 프로토콜상에 인증 및 보안 메커니즘 사용

▷ OSPFv3, RIPng 등에 IPsec 사용
▷ 홉 리미트 (Hop limit) 적용
▷ 6to4와 같은 동적 터널링 보다는 정적인 (Configured Tunnel) 터널링 사용

Ⅳ. 결 론

본 고에서는 IPv6 전환에 따른 여러 가지 보안 고려사항들을 IPv6 프로토콜 자체 이슈와 IPv4/IPv6 연동환경 이슈로 나누어 분석하여 기술하였다. 현재 IPv6는 국내외로 2008년부터 본격적으로 도입되기 시작하여 2010년에는 상용망 구축이 활발해 질것으로 예상되며, 기존 IPv4와의 연동에 대한 요구는 2020년까지는 지속적으로 유지될것으로 보인다. 이때 반드시 요구되는 것 중의 하나는 보안 문제로 현재 표준화 관점과 망 운영 관점에서 하나하나 분석하고 이를 해결하기 위한 연구가 진행중이다. IPv6 보안의 가장 큰 문제는 보안 기술상의 문제가 아니라, 실제 IPv6 상용망을 구축하고 운영해본 경험이 없다는 점에 있다. 실제 IPv6 망을 구축하여 운영하면, 아마도 보안 상의 새로운 문제점들도 계속적으로 보고 될 것으로 믿고 있으며, 이러한 과정이 반복되면, IPv6 역시 보안 관점의 안정적인 차세대 인터넷 상용망으로 빨리 진화될 것으로 믿는다.

참고문헌

[1] E. Nordmark, R. Gilligan, Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213, October 2005.

[2] B. Carpenter, K. Moore, Connection of IPv6 Domains via IPv4 Clouds, RFC 3056, February 2001.

[3] F. Templin, Intra-Site Automatic Tunnel Addressing Protocol(ISATAP), RFC 4124, 2005.

[4] C. Huitema, Teredo: Tunneling IPv6 over UDP through NATs, RFC 4380, February 2006.

[5] J. Bound et al., Dual Stack Transition Mechanism (DSTM), Work-in-progress, 2006

[6] G. Tsirtsis, P. Srisuresh, Network Address Translation - Protocol Translation(NAT-PT), RFC 2766, February 2000.

[7] E. Davies et al., IPv6 Transition/Co-existence Security Considerations, draft-ietf-v6ops-security-overview-04.txt, Work-in-progress, March 2006.

[8] G. Van de Velde et al., IPv6 Network Architecture Protection, draft-ietf-v6ops-nap-02.txt, Work-in-progress, October 2005.

[9] P. Savola, Firewalling Considerations for IPv6, Work-in-progress, draft-savola-v6ops-firewalling-01.txt, March 2003.

[10] F. Dupont, P. Savola, RFC 3041 Considered Harmful, draft-dupont-ipv6-rfc3041harmful-02.txt, work-in-progress, Work-in-progress, January 2003.

[11] P. Savola, Security Considerations for 6to4, RFC 3964, December 2004.

[12] Cisco Systems, IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation(v1.0), 2005.

[13] 신명기, IPv4/IPv6 전환 메커니즘에서의 보안 기술, IT포럼코리아'2006, 2006.

저자소개

신 명 기

2000년 – 2003년 충남대학교 컴퓨터공학과 공학박사
2004년 – 2005년 미국 국립표준기술연구원 (NIST) 초빙연구원
1994년 – 현 재 한국전자통신연구원(ETRI) 차세대 인터넷표준연구팀 선임연구원
2001년 – 현 재 IETF 국제표준화 기구 에디터 (RFC 3338, RFC 4038 등)
2005년 – 현 재 IPv6 Forum CTO Excom 집행위원
주관심분야 차세대인터넷 기술, IPv6, 멀티캐스트, 이동성 관리, IP 보안 기술

용어해설

TCP/IP Offload Engine
TCP/IP Offload Engine, TOE [컴퓨터]

운영체제 내부에서 소프트웨어로 수행되는 TCP/IP 프로토콜 스택을 별도의 전용 하드웨어로 구현한 시스템과 분리된 하드웨어 프로토콜 스택.

수 Gbps급 이상의 네트워크 입출력 처리 속도을 제공하기 위하여 시스템의 TCP/IP 프로토콜 처리 기능을 하나의 하드웨어 장치로 독립시킨 것으로 TOE 하드웨어는 SoC (System on a Chip) 형태로 구현되며 주로 32비트급 RISC(Reduce Instruction Set Computer) 프로세서를 내장하고, 시스템의 공유 자원과 분리되는 독립적인 메모리 공간을 사용한다.

탭 브라우징
tap browsing [기초]

창이 하나의 탭으로 설정되어 여러 개의 창을 열고 탭을 클릭하면서 창을 옮겨갈 수 있는 브라우징.

윈도즈 운영체제를 기본으로 하는 인터넷 익스플로러 브라우저는 마우스 클릭에 대해 새 창으로 뜨는 것을 기본으로 하고 있으나 파이어폭스 같은 운영체제 독립적인 브라우저는 여러 페이지를 하나의 프로그램 창에서 띄울 수 있도록 하고 있다. 인터넷 익스플로러도 7.0 이후에는 탭브라우징 기능이 포함되어 있으며, 기존 브라우저에서도 별도의 프로그램을 이용하면 탭브라우징의 기능을 사용할 수 있다.