IPv6 전환 메커니즘에서의 IPsec 적용 가능성에 대한 연구

김현구*, 임형진*, 홍용근**, 이승윤**, 정태명*
*성균관대학교 전기전자 및 컴퓨터 공학과
전자통신연구원
e-mail:*{hkkim, hjlim, tmchung}@rtlab.skku.ac.kr,
**{yghong, syl}@etri.re.kr

A Study on IPsec Possibility of Adaptation in IPv6 Transition Mechanisms

Hyun-Ku Kim*, Hyung-Jin Lim*, Yong-Gu Hong**,
Seung-Yun Lee** and Tai-M Chung*
*SungKyunKwan University
**Electronics and Telecommunications Research institute(ETRI)

요 약

현재의 IPv4 기반의 네트워크는 사용 가능한 주소 크기의 제약, 취약한 보안 구조 등 여러 가지 문제점을 가지고 있다. 특히 IPv4 프로토콜은 보안 요소를 생각하지 않고 설계되었기 때문에 IPv4 네트워크의 보안을 위해 SSL, IPsec 등 많은 보안 프로토콜 추가로 사용되어 지고 있다. 이러한 문제점을 해결 하기 위해서 IPv6 프로토콜에서는 128 비트의 주소 체계와 더불어 IPsec의 기반의 되는 AH와 ESP 프로토콜을 포함하고 있다. 하지만 IPv6 네트워크로 전환하기 위해서는 기존의 IPv4 네트워크와의 공존이 필요하게 된다. 이러한 이질적인 프로토콜의 공존은 IPv6 IPsec 적용시 문제점을 수반하게 된다. 본 논문에서는 IPv6 전환을 위해 연구되고 있는 여러 메커니즘에서의 IPsec 적용 가능성을 분석하여 IPsec 적용시 발생 할 수 있는 전환 메커니즘에서의 문제점을 도출하고자 한다.

1. 서론

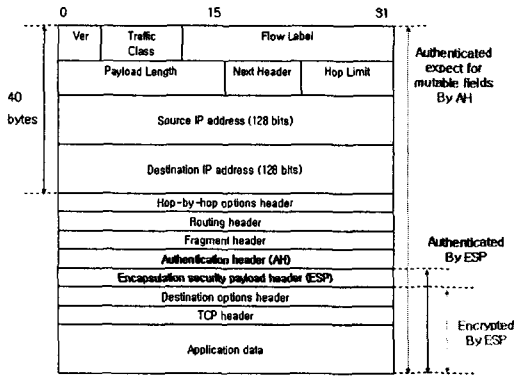
현재 우리가 사용하고 있는 인터넷은 IPv4 기반의 네트워크이다. 이러한 IPv4 주소를 사용한 인터넷 환경은 초기와 달리 네트워크 기술의 급진적인 발달과 인터넷 문화의 급속한 보급으로 인한 폭발적인 사용자 증가, 그리고 사용자들의 다양한 서비스에 대한 요구로 인해 많은 문제점을 나타내고 있다. IETF에서는 이러한 문제점들을 해결하기 위해 IPv6 프로토콜을 제안하였다. IPv6는 IPv4의 주소 고갈 문제를 포함해, 새로 그 중요도가 부각되고 있는 라우팅의 효율성, 이동성 지원, QoS 보장, 자동화된 설정, 보안 기능 등을 포함하고 있다[1,2]. 특히 IPv6의 AH와 ESP 프로토콜은 기존의 IPv4의 부가 보안 프로토콜인 IPsec을 흡수 한 것으로 현재 VPN 방식의 주류를 이루고 있어, 앞으로 높은 활용이 예상된다. 그러나 IPv6가 네트워크 전체에 전개되기까지 상당한 기간동안 현재의 IPv4 네트워크와 공존이 필요하게 될 것이다. IPv6 네트워크로의 자연스러운 전환을 위해서 IETF NGTrans 워킹 그룹을 통해 다양한 전환 메커니즘이 연구 개발되었다[4]. 하지만 이러한 전환 메커니즘의 대부분은 기본 동작만을 정의하고 있을 뿐이다. 순수 IPv4 네트워크나 순수 IPv6 네트워크 만이 존재하는 상황과는 달리 IPv6 네트워크가 전개되어 나가는 과정에서는 IPsec 사용 가능 여부가 전환 메커니즘 선택에 중요한 요소를 작용할 수 있다.

본 논문에서는 이러한 점에 착안하여 IPv6 전환을 위해 연구되고 있는 여러 메커니즘에서의 IPsec 적용 가능성에 대해 비교 및 분석하고자 한다. 본 논문의 2장과 3장에서는 IPv6 AH와 ESP 헤더와 각 전환 메커니즘에 대해 기술하고, 4장에서 각 전환 메커니즘에서의 IPsec AH와 ESP 사용 가능성에 대해 분석을 구체적으로 기술한다.

2. IPv6 IPsec (AH&ESP)

IPv6는 기본적으로 IPv4의 디자인 규칙을 따르고

있으나 헤더의 포맷을 바꾸어, 많은 주소를 포함할 수 있을뿐더러 단순하면서도 유연하게 많은 기능을 가지게 되었다. 이러한 기능은 기본 IP 헤더의 단순화와 덧붙여지는 확장 헤더에 의해 구현되었다. IPv6에서는 이러한 확장 헤더를 통해서 패킷에 대한 부과적인 서비스를 제공한다. 이 중 AH와 ESP 확장 헤더는 IPv6에서 패킷에 대한 인증과 암호화를 수행하는 부분으로 IPv4에서의 IPsec 프로토콜에서와 기능이 같다. [그림 1]은 IPv6 헤더의 형식과 AH와 ESP에 의해 인증되거나 암호화되는 영역을 나타낸다[3].



[그림 1] IPv6 헤더 형식

■ AH 헤더(Authentication Header)

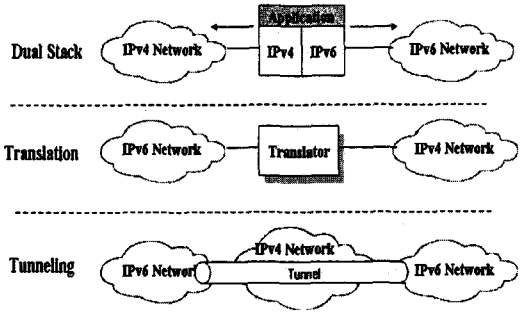
AH는 IP 데이터그램에 대해서 무결성과 데이터 인증, 재전송 공격 방지 기능을 제공한다. 무결성은 메시지 인증 코드로 만들어지는 체크섬에 의해 보장되고, 데이터 인증은 인증된 데이터 안에 포함된 비밀키에 의해 보장된다.

■ ESP 헤더(Encapsulating Security Payload)

ESP는 데이터의 기밀성, 데이터 무결성, 데이터 인증, 재전송 공격 방지 기능을 제공한다. 데이터 기밀성을 제외한 나머지 기능에 대해 AH와 다른 점은 [그림 1]에서와 같이 무결성, 인증에 포함되는 범위이다.

3 IPv6 전환 메커니즘

IPv6의 전환을 위한 메커니즘은 IETF의 NGTrans(Next generation translation) 워킹 그룹을 통해서 연구 및 개발 되었으며, [그림 2]에서와 같이 호스트 관점에서의 듀얼 스택, 게이트웨어 관점인 변환기, 마지막으로 망관점에서 터널링을 이용한 메커니즘으로 분류 될 수 있다[1,4].



[그림 2] IPv6 전환 메커니즘

■ 듀얼스택 (Dual Stack)

IPv6 노드가 IPv4 전용 노드와 호환성을 유지하는 가장 쉬운 방법은 IPv4/IPv6 듀얼 스택을 제공하는 것이다. IPv4 응용은 IPv4 스택을 사용하고 IPv6 응용의 경우에는 IPv6 스택을 사용하여 호환성을 유지하는 방식이다.

■ 변환기 (Translator)

IPv4 전용 노드와 IPv6 전용 노드 사이에 직접적인 통신을 가능하게 하는 것이 IPv4/IPv6 변환 메커니즘의 주 목적이다. 이러한 변환 메커니즘에는 변환이 실제 이루어 지는 계층에 따라 네트워크 계층에서 변환을 수행하는 SIIT[5]와 NAT-PT[7], 수송계층에서 변환을 수행하는 SOCKS[6]와 TRT 시스템[10], 마지막으로 응용계층에서 변환을 수행하는 Squid로 나누어 진다. 또한, IPv4 어플리케이션과 IPv6 어플리케이션을 위한 호스트 기반의 BIS[8]와 BIA[9]가 있다.

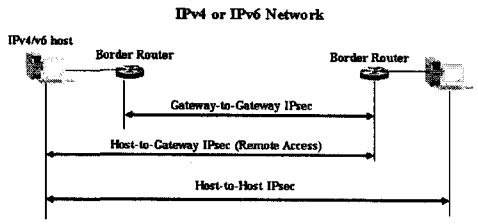
■ 터널링 (Tunneling)

터널링 메커니즘은 기존의 VPN에서와 같이 IPv6 데이터그램을 IPv4 패킷에 캡슐화하여 IPv4 영역을 통과하는 방법을 말한다. 터널링 방법에는 두 노드 간의 IPv4 주소를 통해 매뉴얼하게 터널을 설정하는 방식과 IPv4 주소와 매뉴얼한 설정 없이 IPv6 주소 체계 중 IPv4 주소를 포함하고 있는 IPv6 주소를 이용하여 자동으로 터널링을 하는 방식으로 나누어 줄 수 있다. 이러한 자동터널링 기법에는 IPv4 주소가 IPv6 주소에 어떻게 매핑되는가에 따라서 6over4[13], 6to4[11,12], ISATAP[15]이 있다. 또한 터널 설정을 터널 브로커라는 서버를 통해 자동 관리하는 Tunnel Broker[14], IPv4 데이터그램을 IPv6 패킷에 캡슐화하는 DSTM 메커니즘[16]이 있다.

4. IPv6 전환 메커니에서의 IPsec 적용 가능성

IPv6 네트워크로 자연스러운 전환을 위해서 IETF의 NGTrans 워킹 그룹을 중심으로 전환 메커니즘에 대해 활발한 연구가 진행되고 있지만, 대부분의 경우에서 기본 동작 과정에 대해서만 다루고 있다. 그러므로 패킷의 헤더와 데이터에 따라 인증과 암호화를 수행하는 AH와 ESP 헤더가 사용될 경우 전환 메커니즘이 제대로 동작하지 않는 경우가 생길 수 있다.

IPsec은 AH와 ESP, 동작모드(터널, 수송) 그리고 적용 위치에 따라 다양한 방법으로 사용 가능하다. 여기서는 [그림 3]과 같이 IPsec이 적용되는 대표적인 형태인 Host-to-Host (Pear-to-Pear), Gateway-to-Gateway(Lan-to-Lan), Host-to-Gateway (Remote Access)을 기준으로 IPsec의 사용 가능성을 분류해 각 메커니즘을 분석하였다[4].



[그림 3] IPsec 적용 구간 분류

<표 1>은 현재 연구 중인 전환 메커니즘들에 대한 IPsec 적용 가능성 여부를 앞에서 제시한 적용 구간에 따른 분류에 따라서 정리한 것이다.

<표 1> 전환메커니즘에서의 IPsec 적용 가능성

변환메커니즘		H-to-H		G-to-G		H-to-G	
		AH	ESP	AH	ESP	AH	ESP
Dual Stack		O	O	O	O	O	O
Trans-lator	SIIT	X	△	△	△	X	△
	SOCKS	X	X	△	△	X	X
	NAT-PT	X	△	△	△	X	△
	BIS	△	△	O	O	△	△
	BIA	O	O	O	O	O	O
	TRT	X	X	△	△	X	X
Tunnel	Configured Tunnel	O	O	O	O	O	O
	6to4	O	O	O	O	O	O
	6ovoer4	O	O	-	-	-	-
	Tunnel Broker	△	△	O	O	△	△
	ISATAP	O	O	O	O	O	O
	DSTM	△	△	O	O	△	△

■ 듀얼 스택 메커니즘

듀얼 스택에서는 IPsec이 IPv4 프로토콜과 IPv6 프로토콜이 별도로 적용되기 때문에 IPsec 적용에 제한이 없다. 그렇지만, IPv6 IPsec 설정과 IPv4 IPsec 설정을 모두 가져야 하기 때문에 보안 연계나 키에 대한 관리가 기존의 단일 스택 구현에 비해 복잡하고 어려워 질 것이다.

■ 변환 메커니즘 (Translator)

변환 메커니즘의 경우에는 호스트 기반의 변환 메커니즘인 BIA/BIS와 사이트 기반의 변환 메커니즘으로 나누어서 IPsec 적용 가능성을 생각할 수 있다. 우선 호스트 기반의 BIA는 네트워크 계층보다 상위 계층에서 변환 과정이 이루어지므로 IPsec 적용에 문제가 없고 BIS의 경우에도 호스트 내에서 변환이 이루어지기 때문에 변환기에 IPsec 기능 추가를 통해 사용이 가능할 것이다.

IPsec의 경우 양 종단 간의 네트워크 계층 기반의 보안 설정을 통해 이루어지게 되고, TCP와 UDP 헤더 역시 IPsec에 의해 암호화되거나 인증을 위해 사용 되므로 게이트웨이의 수송 계층에서 변환을 수행하는 SOCKS와 TRT의 경우 호스트에서의 IPsec 사용이 제한된다.

그 외 메커니즘인 SIIT와 NAT-PT 메커니즘 역시 변환이 게이트웨이에서 이루어지게 된다. AH와 ESP 터널 모드의 경우 기본적으로 IPv4와 IPv6는 주소 체계, 헤더 형식과 구성이 다르며 그 크기도 다르기 때문에 IPsec을 위한 보안 연계와 인증 및 암호화 부분 등에서 문제(인증, 암호화 부분 재계산)가 발생하게 되므로 기본적으로 사용이 불가능하다. 이는 IPsec에서의 보안 연계, 인증, 암호화는 패킷의 헤더의 내용, 크기에 영향을 받기 때문이다. 하지만 ESP 수송 모드의 경우 ESP 이전 헤더 영역이 인증 및 암호화 영역에 포함 되지 않기 때문에 부분적으로 사용이 가능 하다.

또한 이러한 변환 메커니즘들 역시 변환 메커니즘이 위치하는 게이트웨이에서부터의 Gateway-to-Gateway (Lan-to-Lan) IPsec의 적용은 가능하다.

■ 터널링 메커니즘 (Tunnel)

Configured 터널, 6to4, 6over4, ISATAP과 같은 터널링 메커니즘은 호스트에서 생성된 패킷이 TEP(Tennel End Point)에서 새로운 헤더와 함께 캡슐화되고 터널의 반대편 TEP에서 디캡슐레이션

되므로 호스트에서 생성된 원본 패킷에는 변화가 없다. IPsec은 보안을 필요로 하는 양 단간의 보안 협상을 통해 패킷 정보를 기반으로 동작을 하기 때문에 IPsec 사용에 문제가 없다. 하지만 Tunnel Broker의 경우에는 듀얼 스택 호스트가 실제 통신에 사용될 IPv6 주소를 터널 브로커에서 동적으로 할당받기 때문에 보안 협상을 자동으로 설정하여 사용하는데는 문제가 생길 수 있다. 그 이유는 보안 협상에 소스와 목적지 주소가 들어 가게 되는데 실제 터널을 요청하기 전에는 호스트가 자신의 IPv6 주소를 알 수 없기 때문에 미리 SA를 설정할 수 없기 때문이다. DSTM의 경우에는 IPv4 패킷이 IPv6로 터널링 되게 된다. IPv4 스택에는 IPsec이 포함되어 있지 않기 때문에 별도의 IPsec 전용 장비나 호스트에 IPsec 클라이언트를 설치해야 한다.

5. 결론 및 향후 계획

지금까지 IPv6 네트워크로의 전환을 위한 전환 메커니즘들에서의 IPsec AH와 ESP의 적용 가능성에 대해 분석하였다. 기본적으로 호스트에서 만든 IPsec 패킷에 변화가 없는 듀얼 스택과 터널링 메커니즘에서는 IPsec 사용에 문제가 없으며, IPv4 전용 노드와 IPv6 전용 노드 사이에 직접적인 통신을 가능하게 변환 메커니즘에 많은 문제점을 나타내고 있다. 이는 IPsec 고유의 특징에서 발생하는 문제점으로 네트워크 주소 및 헤더 정보가 AH와 ESP 인증 및 암호화를 위한 보안 연계 설정이나 실제 인증 및 암호화 과정 중에 사용되기 때문에 무결성과 기밀성을 만족하지 못한다.

향후에는 본 논문에서의 전환 메커니즘에서의 분석을 토대로 여러 전환 메커니즘이 중첩되어 있는 환경에서의 IPsec 적용 가능성과 순수 IPv6 망에서의 AH와 ESP 헤더의 활용 및 적용 시나라오에 대해 연구를 수행 하여, IPv6 네트워크로의 빠른 전환을 위한 토대를 만들 것이다.

참고문헌

[1] 김용진, 박정수, 신명기, 이승윤, "차세대 인터넷 프로토콜 IPv6", 다성출판사, 2002

[2] S. Deering and B.Hiden, "Internet Protocol Version 6 (IPv6) specification", RFC2460, Dec, 1998

[3] S. kent, and R. atkinson, "Security Architecture for the Internet Protocol", RFC2401, Nov. 1998

[4] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC2893, August 2000.

[5] Nordmamark, E., "Stateless IP/ICMP Translator (SIIT)", RFC2765, February 2000,

[6] H.Kitamura, "A SOCKS-based IPv6/IPv4 Gateway Mechanism", RFC3089, April 2001.

[7] Tsirtsis, G. and P. Srisuresh, "Network Address Translation-Protocol Translation (NAT-PT)", RFC2766, February 2000.

[8] K. Tsuchiya, H. Higuchi, Y. Atrarashi, "Dual Stack Hosts using the "Bump-In-the-stack" Technique (BIS)", RFC2767, February 2000.

[9] Seungyun Lee, M-K, Shin, Y-J Kim, E. Nordmark, A. Durand, "Dual Stack Hosts Using "Bump-in-the-API" (BIA)", RFC3338, October 2002.

[10] J. Hagino, K. Yamamoto, "An IPv6-toIPv4 Transport Relay Translator", RFC3142 June 2001

[11] B. Carpenter, K, Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC3056, February 2001

[12] Windows.NET Server2003 IPv6/IPv4 Coexistence and Migration, Microsoft Corporation, August 2002

[13] B.Carpenter, C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicity Tunnels", RFC2529, March 1999

[14] A. Durand, P. Fasano and D. Lento, "IPv6 Tunnel Broker", RFC3053, January 2001

[15] F. Templin, T. Gleeson, M. Talwar and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", draft-ietf-ngtrans-isatap-13.txt, March 2003

[16] Jim Bound, Octavio Medina, Francis Dupont, Hossam Afifi, and Alain Durand. Dual Stack Transition Mechanism (DSTM) , draft-ietf-ngtrans-dstm-08.txt, July 2002