IP 패킷의 안전한 전송을 위한 IP2 프로토콜 설계

양일등°, 이석희, 김성열

청주대학교 컴퓨터 정보공학과

fbiskr@hanmail.net

요약

IETF에서 제정한 IPSec은 현재 널리 사용되고 있는 프로토콜이다. 하지만 패킷의 형태가 스니퍼에 의해 들어날 수 있으면 전문 기술을 가진 기술 집단만이 적절한 응용을 할수 있는 기술이기도 하다. 본 논문은 컴퓨터 통신에서 발생하는 자료를 스니퍼로부터 보호하기 위해 전문 장치의 제안과 IPSec의 대체 프로토콜인 IP2를 제안하고자 한다.

1. 서론

IETF에서 제정한 IPSec은 컴퓨터 통신을 투명하게 보호하기 위해 사용되고 있고, 현재 VPN시장에서 표준으로 자리 잡아 가고 있다[7]. 하지만 상위 프로토콜의 노출과 IPSec사용시 다른 컴퓨터 통신이 사용불가하다는 단점을 가지고 있다. 또한 전문 기술 집단이 아닌 연구 기관에서는 사용에 어려움을 가지고 있는데, 각 OS에서 지원되어야 하며 특정 소프트웨어를 설치해야 하기 때문이다. 이러한 문제점을 해결하기 위해 소규모 외부 장치의 개발을 제안하며 IPSec의 프로 토콜의 복잡성을 감소시켜 구현이 용이하며 상위 프로토콜의 노출을 피할수 있는 IP2(Internet Protocol Protecter)를 제안하고자 한다.

본 논문의 구성은, 2장에서 관련연구에 대한 사항을 기술하고, 3장에서 IPSec에 대한 문제점을 논하고 4장에서 IP2에 대해 제안을 하며 5장에서 결론을 맺는다.

2. 관련 연구

2.1 IPv4

IPv4는 비 연결형 프로토콜로 패킷을 특정 목적지까지 전달하는 기능을 가지며 해당 헤더를 살펴보면 다음과 같다[1].

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment OFfset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

표 1 IP 프로토콜 헤더

IP 프로토콜은 상위 프로토콜로 대표적으로 TCP와 UDP를 지원하는데 IANA(Internet Assigned Numbers Authority : 인터넷 할당 번호 관리 기관)에서 정한 각각의 고유값을 'Protocol' 필드에서 사용하고 있다. 다음 표에 몇가지 프로토콜에 대한 값이 나와 있다[2].

표 2 IANA 프로토콜 번호 요약

Decimal	Keyword	Protocol	References
0		Reserved	[JBP]
6	TCP	Transmission Control	[RFC793,JBP]
17	UDP	User Datagram	[RFC768,JBP]
50	SIPP-ESP	SIPP Encap Security Payload	[Steve Deering]
51	SIPP-AH	SIPP Authentication Header	[Steve Deering]

여기서 TCP는 6, UDP는 17, 그리고 IPSec에서 사용되는 AH(Authentication Header)와 ESP(Encapsulating Security Payload)는 각각 50,51로 나타나 있다.

2.1 IPSec

IPSec은 IETF에서 연구 진행하고 있는 국제 표준 프로토콜로 AH, ESP, IKE(The Internet Key Exchange) 등의 연구를 하고 있다[3].

현재 VPN에서 L2F(Layer 2 Forwardin g Protocol), PPTP(Point to Point Tunne ling Protocol), L2TP(Layer 2 Tunneling

Protocol)등과 함께 사용되어 지고 있으며 대다수의 VPN등이 이를 지원하고 있다[4]. IPSec은 SSL과 같은 프로토콜과는 다르게 시스템에게 투명성을 제공할수 있는데 이는 TCP/IP의 인터넷 계층에서 작동하므로 상위 프로그램의 구조를 수정할 필요가 없기 때문이다.

2.2 AH

AH는 IP 패킷에 대해 인증, 재전송 방지, 무결성 검사등의 서비스를 제공해 주며 사용되는 알고리즘으로는 HMAC-MD5[3.8], HMAC-SHA-1[3.9]이 사용된다[3.5]. AH에는 트랜스포트(transport) 모드와 터널(Tunnel) 모드가 있다.

표 3 AH 헤더 형식

Next Header	Payload Length	RESERVED	
Security Parameters Index(SPI)			
Sequence Number			
Authentication Data			
0	8	16	24

각 모드와 IP 패킷의 결합된 것은 다음과 같이 나타난다.

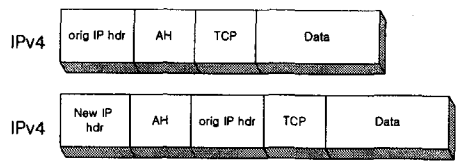

그림 1 트랜스 포트/터널 모드 AH

트랜스포트 모드와 터널 모드의 차이점은 호스트의 TCP/IP 프로토콜 스택에서 직접 처리하는 것과 보안 게이트 웨이(Security Gateway)에서 처리하는 차이가 있고 패킷의 보호 범위의 차이가 있다. SG의 경우에는 해당 네트워크의 길목의 라우터나 방화벽에서 구현이 용이하다.

2.3 ESP

ESP는 IP 패킷에 대해 기밀성, 데이터 출처 인증, 비연결형 무결성, 재전송 방지 등을 제공한다[3.6].

표 4 ESP 헤더 형식

Security Parameters Index(SPI)			
Sequence Number			
Payload Data(variable)			
	Padding	Pad Length	Next Header
Authentication Data(variable)			
0	8	16	24

AH와의 차이점은 데이터 자체에 대한 기밀성에 관한 사항을 주로 다루고 있으며 사용되는 알고리즘으로는 DES/3DES등이 사용되고 있다. ESP에도 트랜스 포트 모드와 터널모드, 두 가지가 있는데 의미는 AH와 같다[3].

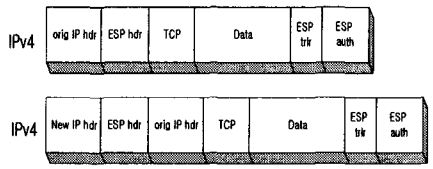

그림 2 트랜스 포트/터널 모드 ESP

3. 문제점

3.1 패킷의 형태 파악

2.1절에서 설명한 IPv4 패킷의 형태를 보면 상위 프로토콜의 형태를 알수가 있는데 이는 스니퍼에 의해 해당 컴퓨터 통신이 IPSec의 AH 혹은 ESP의 사용여부를 판가름하고 offline적으로 정보의 유출 및 online적으로 크래킹을 시도할수 있다.

3.2 IPSec 사용시 다른 컴퓨터 통신 불가

IPSec을 사용할때 해당 컴퓨터와의 통신이외의 통신을 원할 경우(예:yahoo.com)에는 IPSec 기능을 해제하고 사용해야 하는 불편을 초래한다. 이는 구조적인 문제로 인터넷 계층으로 들어가는 패킷의 처리를 모두 해주기 때문에 IPSec을 사용하지 않는 일반 컴퓨터 통신의 경우에는 문제가 될 수 있다.

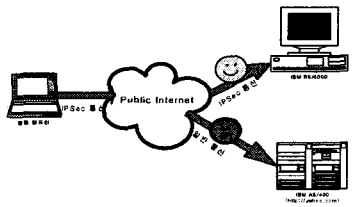

그림 3 인터넷 연결시 문제 관계

3.3 설치상의 문제

현재 일반 사용자들이 IPSec을 접할수 있는 방법은 PC에 설치가능한 소프트웨어인데 그것은 OS의 지원이 반드시 있어야 하는 소프트웨어가 대부분이다.

Microsoft Windows 2000 계열부터와 FreeBSD 계열 및 Linux 계열에서는 FreeS/WAN 이 있는데 Windows의 경우 L2TP와 같이 혼용으로 사용하고 있으며 FreeS/WAN의 경우 커널 패치 및 해당 프로그램을 설치하고 설정을 해야 하는 등 사용이 매우 불편하다. 또한 터널 모드의 사용을 원할 경우 많은 시간과 노력을 투자해야 한다.

4. 설계

4.1 IP2 프로토콜 설계

기본적으로 IP2 헤더, 원본 IP 헤더, IP 데이터 전체를 암호화 하며, 프로토콜의 필드와 함께 암호화 하기 때문에 크래커에 의한 정보 노출의 위험이 없으며, 상위 필드를 재정의 할수 있으므로 정보 보호가 필요치 않는 다른 컴퓨터 통신을 할수 있다.

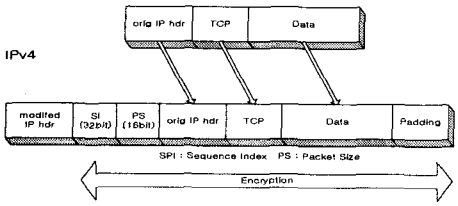

그림 4 IP2 패킷의 구조

IP2 헤더는 다음과 같다.

1) modified IP hdr : Fragment등의 정보가 수정된 후에 헤더에 추가된다.
2) IP2 Version : 4bit 값으로 버전을 나타낸다. 현재 값은 1이다.
3) HFN : 4bit 값으로 헤더 필드의 개수를 나타낸다. 현재 값은 4이다
4) SI : 재전송 방지를 위해 송신자가 일정값을 증가 시키고 수신자가 그 값을 버퍼에 저장하여 검사 하여 재전송 여부를 판가름 하는데 사용된다.
5) PS : 패킷의 사이즈로 IP2의 헤더를 제외한 나머지 부분에서 Padding을 제외한 실제 IP 패킷 사이즈를 가리킨다.
6) CMD : 종단간에 명령을 저장하는 곳으로 명령어, 상위 프로토콜 형식, 사용되는 알고리즘 등이 들어간다.

표 5 CMD 필드 세부 형식

암호화 알고리즘	상위 프로토콜	명령어
DES,3DES,AES	TCP,UDP,ICMP	초기화,전송

7) UP : 상위 프로토콜의 포트번호를 명시한다.
8) Reserved : 미래를 위해 예약되었다.
9) Padding : 복호화 패킷의 크기를 해당 암호화 알고리즘에 맞추기 위해 사용된다.

4.2 쉽게 사용가능한 장치의 제안

장치는 소규모의 전력을 공급할수 있고 100M의 Ethernet을 두개 가지고 있으며 특별한 설정이 필요없는 장치이어야 한다.

4.3 전체 흐름 예상

전체 예상은 아래의 그림과 같으며 세부적인 정보보호 서비스는 다음과 같다.

1. 기밀성, 부인봉쇄 : A 컴퓨터가 데이터를 (A)로 보내면 (A)에서 지정된 키를 가지고 패킷을 암호화 한다. 암호화된 패킷은 Public Network 통하여 (B)로 전송되고 (B)는 지정된 키로 복호화를 하여 B로 전달하기 때문에
2. 접근제어 : C가 A에 접속하려고 시도하면 지정된 규칙에 없기 때문에 접근이 차단된다.
3. 재전송방지 : C가 패킷을 캡처하여 B로 재 전송하게 되면 전송 방지 기능에 의하여 실패한다.
4. 인증 : 자신을 A로 속이고 B에 접속하면 동일한 키로 암호화 된 패킷이 아니기 때문에 인증에 실패한다.
5. 무결성 : 지정된 키로 암호화 된 패킷만 수용되기 때문에 패킷의 내용을 확신할수 있다.

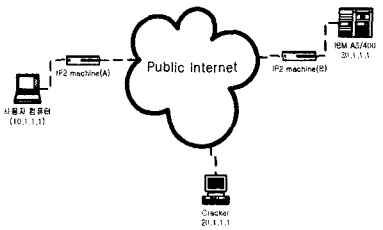

그림 5 컴퓨터 통신 연결 상황

5. 결론

현재 IPv4에서는 선택적이며 IPv6에 기본적으로 채택되어 VPN 및 정보 보호 제품에 많이 사용되고 있는 IPSec에 대한 문제점을 지적하고 새로운 IP2 프로토콜을 제안하였다. 또한 일반사용자들이 쉽게 사용할수 있도록 박스 형태로 제작하여 OS의 종류나 소프트웨어의 종류에 상관없이 사용할수 있는 시스템을 제안하였다.

참고문헌

[1] http://kmh.ync.ac.kr/iguide2/CIE/Cource/Section3/7.htm 2002-8-13

[2] J. Reynolds, J. Postel, "ASSIGNED NUMBERS", RFC 1700, pp. 7-9, October, 1994.

[3] 최용락, 소우영, 이재광, 이임영 공역, "컴퓨터 통신 보안", 도서출판 그린

[4] 박명혜, "VPN(가상사설망)의 기술", 한국전력공사 전력연구원, 2002. 10

[5] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, November, 1998.

[6] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November, 1998.

[7] 최영배, 황성운, 이준석, 윤기송, 김명준, "Introduction to IPSEC(Internet Protocol Security", pp 51-63

[8] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November, 1998.

[9] C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November, 1998.