HMAC를 이용한 IPsec의 Message Authentication Module 설계

김영훈 하진석 이광엽
서경대학교 컴퓨터공학과
e-mail:kylee@skuniv.ac.kr

Design of a IPsec's Message Authentication Module HMAC

Yong-Hoon Kim, Jin-Suk Ha, Kwang-Youb Lee
Dept of Computer Engineering, Seo-Kyeong University

요약

현재 인터넷은 IPv4(Internetworking Protocol, version 4)를 사용하고 있다. 하지만 데이터 통신은 1970년대에 IPv4가 나온 이래에 발전을 거듭하여 왔다. IPv4는 빠르게 발전하는 인터넷에의 요구를 수용하기 위해 IPv6가 제안되었고 현재 표준이 되었다. IPv6에서는 암호화와 인증옵션들은 패킷의 신뢰성과 무결성을 등을 제공한다. 인터넷에서의 정보보호는 인터넷을 구성하는 여러 계층에서 이루어 질 수 있지만, IPsec에서는 AH(Authentication Header)프로토콜과 IPsec ESP(Encapsulating Security Payload)프로토콜 두가지의 암호 프로토콜이 사용되지만 AH에서는 HMAC를 이용한 HMAC-MD5나 HMAC-SHA-1 중 하나를 반드시 기본 인증 알고리즘으로 지원하여야 한다. 본 논문에서는 MD5를 이용한 HMAC-MD5를 기준으로 설계하였으며, Iterative Architecture과 Full loop unrolling Architecture의 두 가지 구조를 설계하였다.

1. 서론

정보 보호의 필요성은 수천 년 전부터 매우 중요한 개념으로 인식되어 왔으며, 상대방의 비밀 정보를 가로채어 자신에게 유리한 정보를 얻고자 하는 노력 또한 경주되어 왔다.

최근 들어서 전 세계적으로 급속히 보급된 인터넷은 이제 인류의 경제생활을 비롯한 모든 활동에 있어서 없어서는 않될 주요 기반구조(infrastructure)의 하나로 자리 잡아가고 있다. 특히 인터넷을 통한, 전자상거래의 확산, 개인간의 통신의 확대, 기업 사설 망의 구축 확산 등으로, 인터넷을 통한 정보 교환 시 정보보호의 중요성은 날로 증대되고 있다.[1]

현재 인터넷은 TCP/IP 프로토콜 중 네트워크 layer의 프로토콜로 IPv4(Internetworking Protocol, version 4)를 사용하고 있다. 비록 IPv4가 설계가 잘 되어 있다고는 하지만 데이터 통신은 1970년대에 IPv4가 나온 이래에 발전을 거듭하여 왔다. IPv4는 빠르게 발전하는 인터넷에 비해 주소공간이 부족하고, 최소지연과 자원의 예약을 요구하며, 정보보호가 필요로하는 분야에서 원하는 데이터의 암호화와 인증을 제공하지 않는다. 이러한 결점을 보완하기위해 IPng(Internetworking Protocol, next generation)이라고도 알려진 IPv6(Internet Protocol version 6)가 제안되었고 현재 표준이 되었다. IPv6는 엄청나게 발전하는 인터넷을 수용하기 위해 많이 수정되었며 IPv6에서는 암호화와 인증옵션들은 패킷의 신뢰성과 무결성을 등을 제공한다. 인터넷에서의 정보보호는 여러 분야에서 여러 가지 암호방식이 사용되고 있으며, 인터넷을 구성하는 여러 계층에서 이루어 질 수 있지만, 디지털 서명분야에는 해쉬함수를 이용한 서명 방식이 널리 이용되고 있다. 해쉬함수는 본래의 메시지를 축약하는 방식으로 이로 인해 디지털서명의 효율성을 높일 수 있다. 즉 디지털 서명 때 해쉬함수에 의해 축약된 메시지를 서명하게 되는데 이로 인해 서명을 위해 필요한 계산, 메모리, 전송량이 크게 줄어든다.

IPsec은 기존 application level에서의 적용되던 보안을 application 과는 독립적으로 보안이 가능하도록 고안된 패킷처리 보안기술로서, 앞으로 VPN(Virtual Private Network)을 구성하는 장비들도 IPsec를 지원할 것으로 추정되고 있다. IPsec에서는 두 개의 protocol(AH , ESP)과 두 개의 mode(turnel , transport)를 지원하는데 protocol 속성은 데이터 패킷이 기밀성 또는 메시지 무결성(또는 둘다)에 의해서 안전한지를 나타내고 mode 속성은 얼마나 많은 데이터 패킷이 승인되어 안전한지를 나타낸다. protocol과 mode의 조합으로 네 개중 하나의 데이터 패킷형태를 선택할 수 있으며 두 프로토콜 모두 무결성을 제공하게 되는데, Message Authentication을 위해 HMAC(Keyed-Hashing for Message Authentication)을 사용한다. MAC는 MDC에 비해 훨씬 느린데 HMAC는 속도의 향상을 위하여 MAC와 MDC를 결합시킨 형태이며 MD5는 SHA-1과 더불어 HMAC에 사용되는 MDC 중의 하나이다. MD5의 취약성에 대해서 연구된 바가 있고 앞으로의 사용에 우려를 표명하는 견해가 있으나 HMAC-MD5에 대해서는 안전한 것으로 결론 짓고 있다.[5]

2. IPsec의 구조

IETF에서는 네트워크 보안 프로토콜의 표준화를 위하여 크게 두 가지 방향으로 진행 중인데, 그림 2.1에서 보는 바와 같이 TCP/IP 프로토콜의 IP layer의 보안을 위한 IPsec과 TCP-Layer 위에서 Server/Client Application 사이에 보안 서비스를 제공하기 위한 TLS(Transport Layer Security)가 있으며, IPsec은 IETF에서 1995년 8월 IPsec을 RFC로 채택된 이후 IPSEC W/G에서 현재까지 표준화가 진행이다. TLS는 현재 널리 이용되고 있는 Netscape사에서 개발한 SSL V3를 개정하여 IETF TLS W/G에서 Internet draft로 채택된 상태이다. 현재 internet에서 이용되고 있는 IP protocol은 packet-switched network에서 단순히 데이터의 신뢰성있는 전송만을 염두에 두고 개발한 것이기 때문에 , 설계당시 보안은 고려되지 않았다. 따라서 IP Spoofing, IP Sniffing과 같은 보안 허점이 생겨나고, 이를 악용하는 경우가 많아지고 있다. 이러한 문제점을 해결하기 위한 방안으로 IP layer에서 보안 서비스를 제공할수 있는 IPsec이 등장하였다.

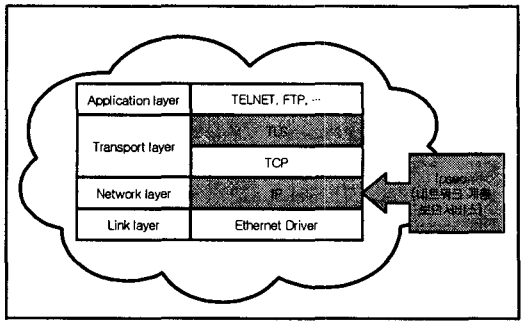


그림 2.1 IPsec과 TLS 프로토콜

IPsec을 통해 제공되는 보안 서비스는 Authentication, integrity, confidentiality, access control, replay attack등의 5가지가 대표적이며, IPsec은 하나 이상의 연결에 대하여 호스트와 호스트사이, 호스트와 보안 게이트웨이 사이, 보안게이트웨이와 보안게이트웨이 사이 세 부분에서 보안 서비스를 제공할 수 있다.

IPsec은 IP-layer에서 다양한 보안 서비스를 제공하기 위한 Security Architecture for the Internet Protocol을 정의하고 있다.

IPsec의 구조는 그림 2.2와 같이 크게 네가지의 구성요소로 나뉜다.

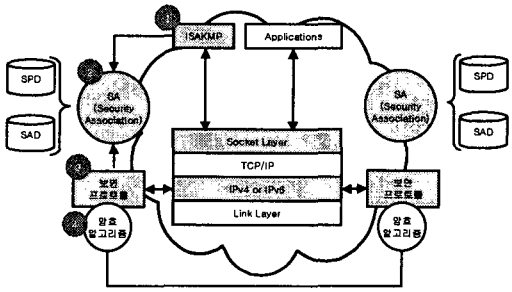


그림 2.2 Security Architecture for the Internet Protocol

IPsec의 구조를 살펴보면 Key Management는 인증과 암호화에 필요한 암호알고리즘의 Key를 생성하고, 분배하기 위한 것으로 ISAKMP(Internet Secrity Association Key Management Protocol)에의해 클라이언트와 Server가 SA를 생성하여 이루어지며, SA는 보안 서비스를 제공하기 우한 프로토콜 각에 대한 매개변수 집합(algorithm ID, Mode, Key, 등)을 정의하고, 관리한는 기능이 요구된다. 이 정보는 개념적으로 SSL의 세션 정보와 동일하다. 보안 프로

토콜(Security Protocol)은 IPsec AH(Authentication Header)프로토콜과 IPsec ESP(Encapsulating Security Payload)프로토콜은 IP-layer에서 보안 서비스를 제공하기 위해 설계된 프로토콜이다. 이러한 프로토콜은 전송모드와 터널모드 두 가지 방식으로 동작할 수 있다. 또한 암호 알고리즘은 제공되는 보안 서비스에 따라 암호 알고리즘은 결정된다.

IPsec에서 SA의 개념은 가장 기본적인 요소인데 IPsec 보안 프로토콜인 AH와 ESP는 모두 SA를 이용하여 보안 서비스를 제공하며, ISAKMP의 가장 중요한 역할은 이러한 SA을 생성하고 관리하는 것이다. 통신하는 두 주체는 연결을 시작할 때 가장 먼저 서로간에 보안 서비스를 제공 기위해 필요한 SA를 상호 협상에 의해서 생성한다. 이때 이러한 SA는 Application마다 독립적으로 생성되어 관리되기 때문에 Security Parameter Index(SPI)와 목적지 주소를 결합하여 ID를 할당함으로써 이용한다.

AH프로토콜은 integrity, data origin authentication, replay attack 방지 등과 같은 세가지 보안 서비스를 제공하기 위해 사용한다. AH DATA형식에 포함된 Authentication Data filed의 값을 계산하기 위해 사용되는 암호알고리즘은 Triple-DES와 같은 대칭키 알고리즘을 기반으로 한 MAC(Massage Authentication Code) 또는 MD5, SHA-1 등과 같은 해쉬 알고리즘을 해쉬 함수를 제공할수 있다. 그러나 IPsec AH 보안 프로토콜은 HMAC-MD5나 HMAC-SHA-1을 반드시 기본 인증 알고리즘으로 지원하여야 한다.[3].[4]

ESP프로토콜은 IP datagram의 Confidentiality, integrity, data origin authentication, replay attack 방지 등과 같은 네가지 보안 서비스를 제공하기 위해 사용한다. 그러나 IP datagram의 기밀성만을 제공하기 위해 이용 될 수 있으며, Payload와 Authentication Data field의 값을 계산하는데 사용되는 암호알고리즘은 보안 연계를 생성할 때 결정되는데 이때 기밀성을 제공하기 위해 ESP는 대칭키 암호 알고리즘을 사용할 수 있도록 설계되었는데 DES-CBC를 반드시 포함해야 하며, 메시지 인증과 부결성을 위해 AH 프로토콜에서 필수로 제공하여야 하는 HMAC-MD5와 HMAC-SHA-1 MAC알고리즘을 이용한다.[2]

3. MD5 회로설계

3.1 HMAC 의 구조

HMAC는 기본적으로 어떤 iterative cryptographic hash function 도 사용이 가능하며,hash function 의 변형없이, 성능 또한 크게 저하되지 않고 사용할 수 있다. HMAC의 구조를 간단히 표현하면 다음과 같다.

HMAC(L) = H(K xor opad , H(K xor ipad, text)

H=cryptographic hash function
K=secret key
ipad = the byte 0x36 repeated B times
opad = the byte 0x5c repeated B times
B = the byte-length of such block
L = the byte-length of hash outputs

즉 , secret key 에 '0'을 덧붙여 B 의 길이로 만든 후(secret key의 길이가 B보다 큰 경우 H(secret key) 가 새로운 key 가 된다) ipad 와 xor 연산을 한다. 연산된 결과에 'text'를 덧붙여 hash function을 적용한 값을 secret key에 opad를 xor한 값에 붙여서 다시 hash function을 적용시킨다. 이때 secret key의 길이가 L보다 작을 경우 보안에 문제가 생길 수 있다.[2]

3.2 HMAC-MD5

본 논문에서는 cryptographic hash function 으로서 MD5를 사용하였으며, MD5는 일반적으로 F,G,H,I 4개의 Function으로 구성 되어있다.

$$F(X,Y,Z) = (X \text{ and } Y) \text{ or } (X \text{ and } Y)$$
$$G(X,Y,Z) = (X \text{ and } Z) \text{ or } (X \text{ and } Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \text{ or } Z)$$

MD5의 구현은 적은 면적을 위한 iterative구조와 빠른 속도를 위한 full loop unrolling구조 두가지로 구현해 보았다.

3.2.1 Iterative Architecture

Iterative 구조는 MD5의 4Round(64step)구성을 공통 부분인 F,G,H,I Function 의 12개의 32bit Register와 8개의 32bit Adder, barrel-shifter부분을 64번의 Looping으로 처리하도록 구조를 설계 하였다. 고정된 부분 즉 Iterractive Core 부분을 제외한 나머지 부분은 FSM(Finite State Machine)을 이용하여 설계하였으며, shifter는 일반적 barrel shifter

의 기능을 축소하였다. 또한 소형크기의 코어에 맞추어 2bit mux를 이용하여 Left Rotate shifter만을 구현하였으며, Adder는 면적과 속도 위하여 일반적인 Ripple-Carry Adder를 사용하여 구현하였다.

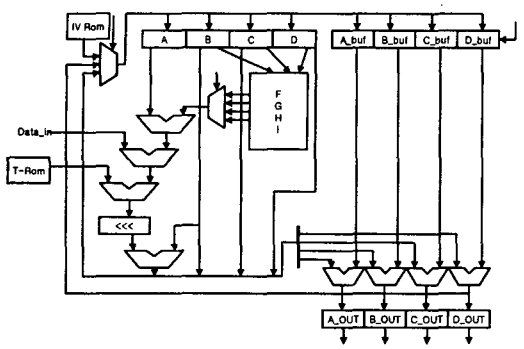
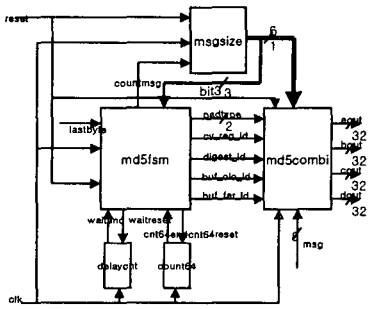


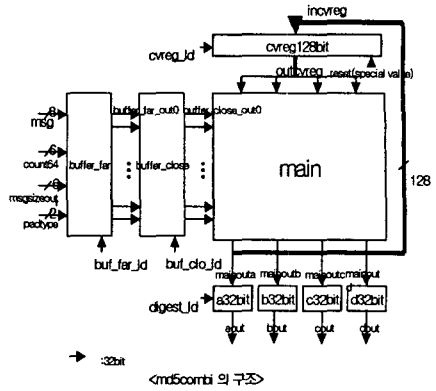
그림 3.1 Iterative Core 구조

3.2.2 Full loop unrolling Architecture



<Full loop unrolling Architecture>

full loop unrolling 구조는 MD5의 4round(64step)을 combination logic으로 설계한 것으로서, Iterative Architecture를 64step 모두를 공통부분 없이 순서대로 나열하여 보다 빠른 logic으로 설계 하였다. 또한 MD5의 초기과정인 padding과 appending length 도 내부에 포함하여 software의 부담을 줄이고 보다 독립적으로 동작하도록 하였다. Iterative Architecture에서 필요하였던 barrel shifter는 combination logic에서 직접 shifting 한 값을 할당해 줌으로서 제거할 수 있고, padding 부분은 message 가 입력될 때 counter가 lastbyte 신호에 따라 counting을 멈추게 함으로써 message를 byte 단위로 count하며 그에 따라 "1000...00"을 할당하였고 appending length는 count된 byte 수를 3bit left shift 하여 append하였다.



<md5combi 의 구조>

4. 결론

본 논문에서는 IPv6에 포함된 IPsec의 authentication으로서 사용되는 HMAC구현에 있어서 MD5를 Cryptographic hash function 으로 사용하여 Iterative 와 Full loop unrolling architecture 두 가지로 설계하였다. 설계와 Simulation은 Synopsys와 Xillinx-Foundation3.1을 이용하여 설계하였으며, Interactive는 vertex-XCV800HQ-240(80만 Gate)에서 Utilization이 5%의 Size를 가지며, 동작 주파수는 10Mhz이다. Full loop unrolling은XCV800HQ-240(80만 Gate)에서 Utilization이 slice 5065/9408로 58%의 size를 가지며, 동작 주파수는 50Mhz로 동작한다.

→본 논문은 시스템 2010사업과 부분적으로 IDEC 지원장비로 작성됨

참고문헌

[1] ETRI, "암호학의 기초", 경문사, 1999년 03월.

[2] William Stallings, "Cryptography And Network Security" second edition, prentice hall, 1998

[3] 이만영 외 공역, "전자상거래 보안기술", 생능출판사, 1999.8

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

[5] H. Dobbertin, "The Status of MD5 After a Recent Attack", RSA Labs' CryptoBytes, Vol. 2 No. 2, Summer 1996.

[RFC-2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC-1321] Rivest, R., "MD5 Digest Algorithm", RFC 1321, April 1992. [ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload", RFC 2406, November 1998.