가상 사설망을 이용한 홈 네트워크의 보안 설계 및 구현

김상현*, 김상욱

*경북대학교, 정보보호학과

Security of Home Network using Virtual Private Network

Sang-hyun Kim*, Sang-wook Kim

*Department of Information Security, Kyungpook National University

요 약

본 논문에서는 이동 단말기를 이용해 외부 네트워크에서 홈 네트워크로 안전하게 접근을 하기 위한 방법을 제시한다. PDA(Personal Digital Assistants)와 같은 이동 단말기가 발달함에 따라 외부 네트워크에서 홈 네트워크에 접속하여 가전 장비들을 제어하는 연구가 매우 중요하다. 그러나 방화벽만으로 홈 네트워크의 장비에 안전하게 접속하여 제어하기에는 많은 문제점을 지니고 있다. 본 논문에서는 외부네트워크에서 홈 네트워크로의 안전한 접근을 위해서 가상 사설망(Virtual Private Network)을 홈 네트워크에 적용하는 방법을 제시한다.

Ⅰ. 서론

홈 네트워크에 있는 가전 기기들을 외부 네트워크에서 제어하기 위해서는 보안의 사각지대 라고 할 수 있는 인터넷에 반드시 연결이 되어 있어야만 한다. 따라서 PDA와 같은 이동 단말기를 이용하여 외부 네트워크에서 홈 네트워크에 접근하여 이런 가전 장비들을 안전하게 제어하기 위한 연구가 매우 중요하다.

그러나 기존의 시스템에 많이 사용하고 있는 방화벽만으로 안전하게 접근 및 제어하기에는 많은 문제점을 지니고 있다. 방화벽은 주로 IP 패킷의 발생지 주소를 보고 내부 네트워크로의 진입 여부를 판단하기 때문에 이를 이용하여 이동 단말기의 외부 네트워크에서 홈 네트워크의 접근을 제어한다는 것은 거의 불가능하다. 이를 해결하기 위해서 최근에 가상 사설망을 이용한 접근 제어 기술이 큰 관심을 받고 있다. 그러나 현 시장에 나와 있는 대부분의 제품들은 하드웨어 장치를 이용한다. 큰 네트워크 트래픽이 오가는 기업이나 기관들 간의 통신에 보안성을 제공하기 위해서는 이러한 제품들이 효용성을 가질 수 있지만 홈 네트워크와 같이 외부 네트워크에서의 트래픽이 그다지 크지 않는 곳에서는 오히려 자원의 낭비를 초래한다.

따라서, 본 논문에서는 이러한 문제점들을 해결하고 PDA와 같은 이동 단말기를 이용하여 외부 네트워크에서 홈 네트워크의 가전 장비들을 안전하게 접근 및 제어하기 위해서 소프트웨어적 가상 사설망 기술을 연구 개발한다.

본 논문의 제 2장에서는 가상 사설망 기술과 가상 사설망에 사용 될 SEED대칭키 블록 암호 알고리즘, MD5 해쉬 함수 알고리즘에 대해서 설명한다. 3장에서는 소프트웨어 가상 사설망을 이용한 홈 네트워크 보안에 대해서 설명하고, 제 4장에서는 구현 모습을 보이고 제 5장에서는 결론을 맺는다.

Ⅱ. 가상 사설망, SEED 및 MD5

1. 가상 사설망

가상 사설망은 인터넷과 같은 광역 네트워크(Wide Area Network)에서 사설망과 같은 보안성을 제공하기 위해서 소개가 되었다. 가상 사설망 서비스의 종류는 3가지로 나누어 볼 수 있다. 여러 지역에 위치에 있는 로컬 지역 네트워크들을 상호연결하기 위한 로컬 네트워크 상호연결 가상 사설망 서비스(LAN interconnect VPN services), 이동 단말기 및 전화 접속을 위한 다이얼업 가상 사

설망 서비스(Dial-up VPN services), 마지막은 위의 두 가지를 결합하여 광역 네트워크에 사용할 수 있는 익스트라넷 가상 사설망 서비스(Extranet VPN service)이다.[1]

또한 가상 사설망에 사용되는 프로토콜은 크게 3가지로 나누어진다. IETF(Internet Engineering Task Force)에서 개발해서 유지하고 있는 IPsec은 네트워크 계층에서의 보안성을 제공한다. AH(Authentication Header), ESP(Encapsulation Security Payload), IKE(Internet Key Exchange)와 암호 알고리즘을 이용하는 IPsec은 인증, 기밀성 및 부인 봉쇄 등의 보안성을 제공한다. 마이크로 소프트사를 주축으로 한 컨소시엄에서 개발된 PPTP(Point-to-Point Tunneling Protocol)은 IP 패킷 안에 PPP(Point-to-Point Protocol) 패킷을 암호화하여 보안성을 제공하는 것으로 마이크로 소프트사의 암호 알고리즘 MPPE(Microsoft Point-to-Point Encryption)을 사용한다. L2TP(Layer 2 Tunneling Protocol)은 인터넷 서비스 공급자에게 다이얼업 접속을 한 사용자의 연결을 터널링하여 보안성을 제공한다. 이 터널링은 LAC(L2TP Access Concentrator)와 LNS(L2TP Network Server)를 이용하여 이루어진다.[2]

2. SEED 및 MD5

1) SEED

SEED는 정보보호진흥원에 개발한 것으로 128bit 대칭키 블록 암호 알고리즘의 국내 표준이다.

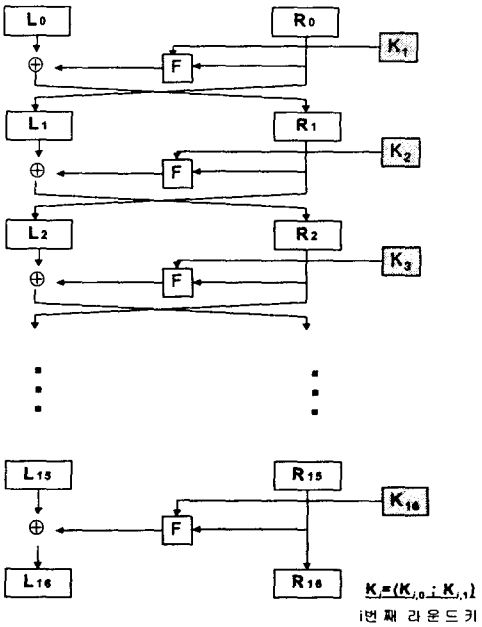

그림 1 : SEED 전체 구조도

위의 그림1은 SEED의 전체 구조 도를 나타낸다. 128비트 입력 평문 블록을 2개의 64비트 블록 $(L_0(64), R_0(64))$으로 나누어, 16개의 64비트 라운드 키를 이용하여 16라운드를 수행한 후, 최종 128비트 암호문 블록 $(L_{16}(64), R_{16}(64))$을 출력하는 것을 보여 준다.[3]

2)MD5

MD5는 인터넷 표준으로 임의의 길이의 메시지를 받아서 128bit의 메시지 다이제스트(Message-Digest)를 출력하는 해쉬(hash) 함수이다. MD5는 같은 메시지 다이제스트를 가지는 두 메시지가 존재하는 것은 거의 불가능함을 이용하여 인터넷에서 무결성 검사를 위한 값으로 많이 사용된다. [4]

MD5는 다음의 5단계를 이용하여 메시지 다이제스트를 만든다.

- 확장 비트(bits) 추가
- 원본 메시지의 길이 추가
- MD 버퍼 초기화
- 16개의 워드 블록에서 메시지 처리
- 메시지 다이제스트 출력

Ⅲ.VPN을 이용한 홈 네트워크 보안

홈 네트워크 장비들의 보안 제어를 위해서 기존의 방화벽으로 제어 시 문제점들과 하드웨어 가상 사설망의 부적합성을 해결하기 위하여 본 논문에서는 소프트웨어 가상 사설망을 적용하여, 외부 네트워크에 위치한 PDA에서 홈 네트워크 가전기기들을 안전하게 접속하기 위한 방법을 제시한다. 홈 네트워크 보안을 위한 전체 개요는 그림 2와 같다.

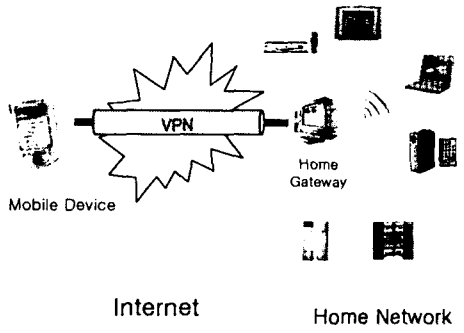

그림 2 : 전체 개요도

위의 그림2는 PDA를 이용하여 홈 게이트웨이에 안전하게 접속하기 위하여 가상 사설망을 이용하는 것을 보여준다. 그러나 현 시중에 나와있는 대부분의 가상 사설망 제품들은 하드웨어 장치를 이용한다. 기업이나 기관들간의 통신 등 네트워크 트래픽이 많은 통신에 보안성을 제공하기 위해서는 하드웨어 장비들을 이용한 가상 사설망이 효용성을 발휘할 수 있다. 하지만 홈 네트워크의 특성상 네트워크 트래픽이 그렇게 많지가 않고 암호 알고리즘을 소프트웨어적으로 빠르게 처리하기 위한 많은 방법들이 나와 있어 홈 네트워크에서는 하드웨어 장비를 사용하는 것은 오히려 자원의 낭비를 가져온다. 또한 이동 단말기는 이동성을 보장해야 되기 때문에 하드웨어 가상 사설망은 적합하지가 않다. 따라서, 본 논문에서는 IPsec를[5] 참조한 응용 계층에서의 소프트웨어 가상 사설망을 개발한다.

소프트웨어 가상 사설망을 개발하기 위하여 IPsec을 사용할 경우 커널 소스 코드의 IP 스택 부분을 수정하거나, 지나가는 패킷을 IP 하부 레이어 에서 캡쳐하기 위하여 새로운 네트워크 드라이버를 만들어야 한다. 하지만 이것은 오히려 오버 헤드가 더 클 수 있기 때문에 본 논문에서는 응용 계층에서 새로운 프로토콜을 디자인하여 응용 계층에서의 가상 사설망을 제공한다.

Type	Error code	Sequence Number
Payload		
Payload		
Integrity Checking Value		

Type	Error code
0 - user authentication	0 - Invalid user
1 - user add	1 - Not authenticated
2 - user delete	2 - Connection closed
3 - authenticated	3 - Invalid data

그림 3 : 프로토콜 구조

위의 그림3은 응용 계층에서 사용 할 프로토콜의 구조를 나타낸다. 타입 필드는 8비트로 메시지의 타입을 , 다음 8비트인 에러 필드에서는 에러가 발생 시 에러 메시지를 표시하기 위한 에러코드, 16비트 크기의 시퀀스 넘버 필드에서는 리플레이(replay) 공격을 막기 위한 시퀀스 넘버를 표시한다. 다음의 페이로드 부분은 SEED 블록 암호 알고리즘을 사용하여 전송할 메시지를 암호화하여 저장하는 부분을 나타낸다. 마지막 필드는 MD5를 사용하여 생성된 무결성 검사 값을 저장하는 부분으로 128비트의 크기를 가진다. 즉 송신 측에서 메시지를 암호화하고 이 암호화 된 값을 이용하여 메시지 다이제스트 값을 만든 후 전송하면 수신 측에서는 먼저 메시지 다이제스트 값을 이용하여 무결성 여부를 검사하고 이상이 없으면 암호 알고리즘으로 복호화 하여 원본 메시지를 추출하게 된다.

Ⅳ. 구현

본 논문에서는 PDA용 운영체제로 Windows CE 3.0을 사용한다. 홈 게이트웨이와의 통신용 PDA 클라이언트 프로그램은 Embedded Visual C++ 3.0을, 홈 게이트웨이에서 작동하는 서버 프로그램과 Visual C++ 6.0을 사용한다.

PDA의 개발 환경은 다음과 같다. CPU는 MIPS VR4122 150MHz 64bit RISC CPU를 사용하고 32MB의 RAM과 16MB의 ROM을 사용한다. 또한 240x320 픽셀,TFT(65536칼라)와 터치스크린 , USB, IrDA 1.2 (115.2 Kbps Max), CompactFlash Card, 3.3V Type I, II , Speaker, Stereo Earphone Jack (3.5mm), Microphone 등을 사용한다.

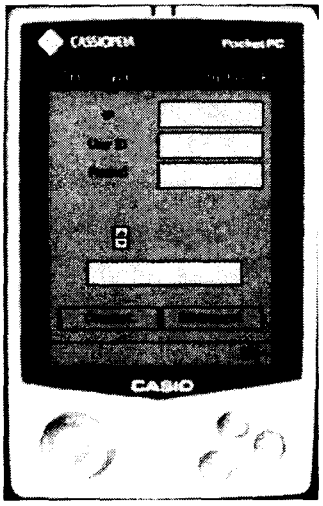

그림 27 : 구현 모습

위의 그림 4는 구현 모습을 나타낸다. IP 주소와 사용자 아이디 패스워드를 입력 후 접속을 하면 사용자 인증을 하게되고 올바른 사용자가 아니면 에러 메시지를 화면에 표시한다. 타당한 사용자이면 더 이상의 인증 과정 없이 인증 과정에서 사용한 정보를 이용하여 암호화하여 통신을 하게 된다.

V. 결과

본 논문에서는 홈 네트워크 기기들을 외부 네트워크에서 PDA등의 이동 단말기를 이용하여 안전하게 접속하기 위한 방법을 제시한다. 기존의 방화벽으로 제어시의 문제점과 하드웨어 가상 사설망을 홈 네트워크에 사용 시 부적합성을 해결하기 위하여 응용 계층에서 새로운 프로토콜을 디자인하여 소프트웨어 가상 사설망을 구현하였다.

향후 연구 내용은 보다 다양한 암호 알고리즘을 제공하고 비밀키를 안전하게 교환하기 위하여 프로토콜의 확장 및 SA(Security Association)[6]를 추가하는 것이다.

참고문헌

[1] R. Venkateswaran, "Virtual private networks", IEEE Potentials , Volume 20, Issue 1 ,pp11-15, Feb-March 2001

[2] Adam Quiggle, Implementing Cisco VPNs:A Hands-on Guide, Osborne/McGraw-Hill, 2001

[3] www.kisa.or.kr

[4] RFC-1321

[5] www.ietf.org

[6] RFC-2401prop