VPN을 위한 응용 계층에서의 새로운 보안 프로토콜 설계 및 구현

김상현*° 백병욱 강철범 배현철* 김동필* 박인성 김상욱
경북대학교 정보보호학과*, 컴퓨터 과학과
{shkim°, bwback,cbkang,dpkim,hcbae,ispark,swkim}@woorisol.knu.ac.kr

Design and Implementation of new Protocol to Provide VPN in Application Layer

Sanghyun Kim*° Byungwook Back Chulbum Kang Hyunchul Bae* Dongphil Kim* Insung Park
Sangwook Kim
Dept. of Information Security* and Computer Science, Kyungpook National University

요 약

본 논문에서는 안전한 데이터 통신을 제공하기 위하여 응용계층에서 새로운 프로토콜을 설계 및 구현한다. 인터넷의 급속한 전파와 더불어 웜, 바이러스, 해킹 등 이를 이용한 많은 보안상의 위협을 받고 있다. 이런 위협으로부터 두 노드간의 데이터 통신을 안전하게 보호하기 위한 연구는 반드시 행해져야만 하고 또한 많은 연구가 진행되고 있다. 이런 연구의 일환으로 본 논문에서는 보안성을 제공하고 있는 다른 프로토콜들의 문제점들을 보완하고 두 노드간의 안전한 데이터 통신을 제공하기 위하여 응용계층에서 새로운 프로토콜을 설계 및 구현한다.

1. 서 론

인터넷 산업의 발전에 힘입어 몇 년 사이 인터넷의 사용이 급속도로 증가하였다. 이로 인하여 우리 생활 자체도 많이 편리해 졌을 뿐만 아니라 많은 변화도 가져 왔다. 하지만 이로 인한 병폐도 그 발전 속도만큼이나 증가 하게 되었다. 웜, 바이러스, 각종 시스템 해킹 등의 악의적인 행동으로 개인 사생활 침해 및 네트워크 서비스 시스템을 다운시키는 것 등이 그 대표적인 예이다. 이런 병폐로부터 사용자들을 보호하기 위한 연구는 반드시 필요할 뿐만 아니라 지금 현재 많은 연구가 진행 중이다. 따라서 본 논문에서는 이런 연구의 일환으로 데이터 통신에 보안성을 제공하기 위하여 현재 많이 사용하고 있는 몇 몇 프로토콜들의 문제점들을 보완하고 보다 안전성 있는 데이터 통신을 제공하기 위하여 응용 계층에서 새로운 프로토콜을 설계하고 구현한다.

현재 많은 주목을 받고 있는 가상 사설망의 프로토콜로 주로 사용되는 것은 IPsec[1] 프로토콜이다. IPsec은 네트워크 계층에서 보안성 있는 통신을 제공하기 위하여 개발된 것으로 기업체나 기관등 대규모 네트워크 사이에서 가상적인 사설망을 제공하기 위하여 게이트웨이에서 많이 사용된다. 이런 가상 사설망은 게이트웨이에서 게이트웨이 사이에 보안 채널을 형성하여 강력한 보안 기능을 제공하지만 게이트웨이와 내부 네트워크의 호스트 사이에는 보안성을 제공하지 못한다. 또한 게이트웨이에서 모든 암호 알고리즘을 처리하기 때문에 트래픽 량이 많은 경우 게이트웨이에 많은 과부하가 걸리게 된다.

웹 애플리케이션의 보안을 위해 많이 사용되고 있는 SSL(Secure Socket Layer)[2]은 넷스케이프사에서 개발한 프로토콜로 데이터 암호화, 서버 인증, 메시지 무결성 검사 및 클라이언트 인증 등의 보안을 제공한다. 이 프로토콜은 레코드 프로토콜과 핸드 쉐이크 프로토콜의 두 개의 레이어로 되어 있다. 레코드 프로토콜에서는 해쉬 함수와 비밀 키 암호 알고리즘을 사용하지만 핸드 쉐이크 프로토콜에서는 공개키 암호 알고리즘을 사용한다. 따라서 네트워크 트래픽량이 많은 경우 공개 키 암호 알고리즘의 많은 계산량 때문에 퍼포먼스가 많이 떨어지게 된다. 특히 PDA와 같이 자원이 제한된 모바일 장치에서는 더더욱 퍼포먼스가 떨어지게 되어 적용하기가 힘들게 된다.

따라서 본 논문에서는 엔드 투 엔드 사이 전체에 보안 채널을 형성하여 안전한 데이터 통신을 제공하고, PDA와 같은 모바일 단말기에서도 유용하게 사용할 수 있도록 하기 위하여 응용 계층에서 새로운 프로토콜을 설계 및 구현한다.

본 논문의 제 2 장에서는 본론에서 사용하게 될 암호 알고리즘인 SEED[3]와 해쉬 함수인 MD5[4]에 대해서 알아보고 , 제 3 장에서는 보다 자세하게 프로토콜에 대하여 설명을 한다. 제 4 장에서는 프로토콜을 이용한 통신의 구현 모습을 보이고 제 5 장에서는 결론을 맺는다.

2. SEED 및 MD5

2.1 SEED

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

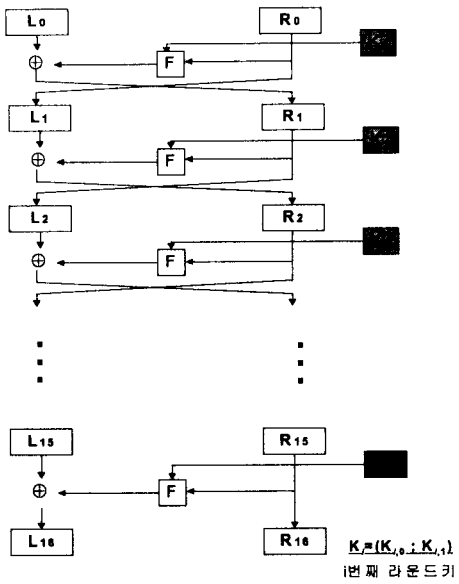

그림 1 : SEED 전체 구조도

위의 그림1은 SEED의 전체 구조도를 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.

2.2 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.
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[5]

3. 응용 계층에서의 새로운 프로토콜

앞서 설명한 것처럼 가상 사설망의 프로토콜로 많이 사용되는 IPsec 프로토콜은 엔드 투 엔드 사이에서의 안전한 데이터 통신은 제공하지 못한다. 또한 웹 애플리케이션의 보안을 위해서 많이 사용되는 SSL은 공개 키 암호 알고리즘을 사용하기 때문에 PDA와 같은 모바일 단말기에는 적합하지 못하다.
비슷한 보안성을 제공하면서 위의 문제점들을 보완하기 위하여 본 논문에서는 응용 계층에서 새로운 프로토콜을 설계 및 구현 하였다. 아래의 그림은 이 프로토콜의 구조를 나타낸다.

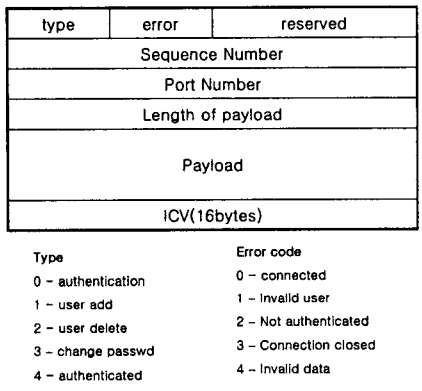

그림 2 : 프로토콜의 구조

타입 필드는 데이터 통신의 타입을 나타낸다. 0은 사용자 인증 과정을 나타내고, 1은 사용자의 새로운 추가, 2는 등록된 사용자의 삭제 시 사용된다. 3은 사용자의 패스워드 변경 시 사용되고 마지막 4는 인증 과정후의 데이터 통신을 나타낸다. 여기서 사용자 추가 및 삭제는 관리자 많이 사용할 수 있다.
에러 필드는 에러 메시지를 화면에 보여주기 위하여 사용된다. 0은 인증 과정이 끝난 후에 연결이 이루어졌을 때를, 1은 등록된 사용자가 아닌 경우를, 2는 패스워드가 틀렸을 경우를, 3은 무결성 검사 시 에러가 발생했을 경우나 해당 사용자의 비밀 키가 아닌 키로 암호화나 복호화를 수행했을 경우를 나타낸다. 마지막 4는 위의 1,2,3의 이유로 인해 연결이 끊어졌음을 나타낸다.
시퀀스 넘버 필드는 리플레이 공격을 막기 위한 필드로 인증 과정 후 서버에서 랜덤 넘버를 생성하여 클라이언트에 보내고 이를 받은 클라이언트는 랜덤 넘버에 1을 더하여 다시 서버에 보내게 된다. 이후 통신은 계속해서 1씩 추가하며 통신을 하게 된다.
포트 넘버는 인증이 된 후에 클라이언트와 통신을 하기 위해서 열어놓는 서버의 포트 넘버이다. 먼저 인증 과정이 성공적으로 끝난 후에 서버에서는 랜덤 포트 넘버를 생성하여 클라이언트에게 보내게 된다. 이를 받은

클라이언트는 이 포트 넘버로 서버에 접속을 하여 계속해서 데이터 통신을 하게 된다. 이와 시퀀스를 넘버를 같이 이용하면 보다 강력하게 리플레이 공격을 막을 수가 있게 된다.

패이로드 길이 필드는 패이로드의 길이를 나타내는 것으로 복호화시 패이로드를 추출할 때 사용된다.
패이로드 부분은 실제로 주고받는 메시지들이 들어가는 부분으로 통신의 타입에 따라 그 내용이 달라진다.

마지막 무결성 검사 값 필드는 데이터 통신 시 무결성 검사 값을 체크하기 위하여 MD5에 의해서 생성된 메시지 다이제스트가 들어가게 된다.

실제 통신 과정은 아래 그림의 연결 과정과 같다.

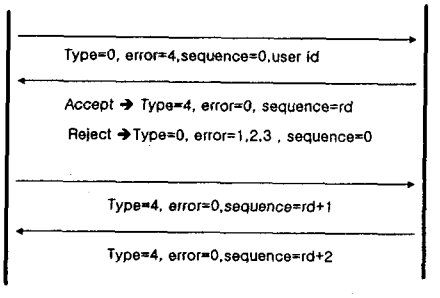

그림 3 : 연결 과정

먼저 클라이언트에서 타입 필드를 0, 에러 필드를 4, 시퀀스 넘버를 0으로 세팅하고 사용자 아이디를 패이로드에 넣은 후에 모든 필드들을 SEED 암호 알고리즘으로 암호화를 한다. 다음 암호화된 데이터를 MD5의 입력 값으로 넣어 메시지 다이제스트를 만든 후 암호화된 데이터의 끝에 추가하여 보내게 된다. 다음 서버에는 보내온 암호화된 데이터를 이용해 메시지 다이제스트를 만들어 보내온 메시지 다이제스트와 비교해 이상이 없으면 복호화를 하고 수용 메시지를 보내서 계속해서 데이터 통신이 이루어지고, 이상이 있으면 에러 메시지와 함께 거부 메시지를 보내서 연결을 닫게 된다.

이와 같이 응용 계층에서의 새로운 프로토콜을 이용하여 프로토콜 자체 내에서 사용자 인증, 데이터 무결성 검사, 전달되는 메시지의 암호화 등의 보안성을 제공하게 된다.

4. 구 현

위의 프로토콜을 이용하여 사용자 인증, 무결성 검사, 전달 메시지의 암호화, 복호화 등을 구현해 보았다. 개발 환경은 클라이언트 프로그램은 마이크로소프트의 EVC++ 3.0을, 서버 프로그램은 VC++ 6.0을 사용하였다.

아래의 그림은 PDA 에뮬레이터에서 작동중인 클라이언트 프로그램과 일반 PC 데스크 탑에서 작동중인 서버 사이의 통신을 보여준다.

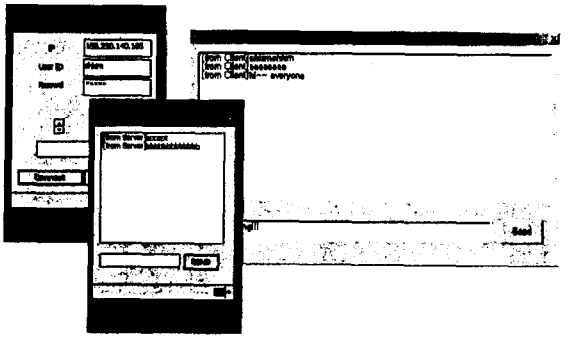

그림 4 : 인증 과정후의 통신

5. 결 론

본 논문에서는 엔드 투 엔드 사이의 안전한 데이터 통신 및 PDA와 같은 이동 단말기에서도 보안성 있는 통신을 제공하기 위하여 응용 계층에서 새로운 프로토콜을 설계 및 구현 하였다.

향후 과제는 보다 안전성을 높이고 이동 단말기에서의 퍼포먼스를 향상시키기 위하여 타원 곡선 알고리즘을 이용한 암호화 및 인증 기능을 추가하고자 한다.

[참고 문헌]

[1] www.ietf.org
[2] wp.netscape.com/security/techbriefs
[3] www.kisa.or.kr
[4] RFC-1321
[5] 김상현, 김상욱, "가상 사설망을 이용한 홈 네트워크의 보안 설계 및 구현," 정보보호학회 학술대회 논문집, 제 12권, 1호, pp27 - 30, 2002년 11월