무선 인터넷 보안을 위한 SSL 활용 연구

김기욱*, 정경훈*, 장용호**, 김창수*
부경대학교 전자계산학과*
부경대학교 전산정보학과**

A Study on the Application of SSL for Wireless Internet Security

Ki-Uk Kim*, Jung Kyung-Hoon*, Young-Ho Jang; Chang-Soo Kim***
Dept. of Computer Science, PuKyong Nat'l University*
Dept. of Computer Science and Information, PuKyong Nat'l University**
E-mail : kimkiuk@mail1.pknu.ac.kr, cskim@pknu.ac.kr

요 약

최근 무선 인터넷을 이용한 전자 상거래가 증가하고 있으며, 이에 따라 무선 인터넷 환경에서의 보안에 관한 관심이 집중하고 있다. 본 연구에서는 무선 인터넷 프로토콜별 보안 서비스를 분석한 후, 현재 유선에서 많이 활용되고 있는 128bits SSL 보안 프로토콜을 무선에서 적용하기 위한 활용방안에 대해 연구한다. 그리고 무선 SSL-Proxy의 기능에서 다양한 응용 계층의 프로토콜과의 호환성 기능들에 대해 고찰한다.

1. 서론

무선 인터넷은 사용자가 이동중 무선 단말기와 무선망을 이용해서 인터넷 서비스를 제공받을 있는 환경과 기술을 말한다. 국내 무선 인터넷 사업은 1999년 초 이동통신전화 사업자를 중심으로 추진되기 시작하였고, 2000년에는 망사업자, 솔루션 및 컨텐츠, 그리고 무선 단말기 공급업체까지 참여하면서 국내 무선 인터넷 사업은 활기를 띠기 시작하였다. 최근 무선 인터넷이 각광을 받고 있는 이유는 우선 IMT-2000서비스로 인한 데이터 전송 속도의 증가를 꼽을 수 있다. 즉, IS-95 및 95A 규격에 근간한 이동통신방식은 최대 14.4Kbps까지 전송속도가 가능하였지만 2000년 12월 도입된 IS-95C서비스는 144kbps까지의 전송속도가 가능하여 이동통신망과 휴대 단말기를 통한 동영상 및 고속 무선 인터넷 서비스의 제공을 가능하게 하였다. 둘째는 기존의 고정된 환경에서의 유선 인터넷과는 달리 무선 인터넷은 이동 통신단말기를 사용함으로써 언제 어디서나 인터넷 접속이 가능하다는 무선 인터넷 사용의 휴대성을 들 수 있다. 그리고 세 번째는 무선 인터넷 시장기회 확대에 있다. Golbal Mobile보고서에 의하면 2001년까지는 무선전화 가입자수가 약 6억 명에 달할 것이며, 이미 무선 인터넷 사용자는 세계적으로 6백만 명이 넘었고, 우리나라의 경우만 10~20만 명으로 추산하고 있다[1]. 마지막으로 프로토콜의 표준화 경향이다. 즉, WAP포럼 가입 회사들을 중심으로 한 WAP방식과 Microsoft와 Qualcomm연합의 Mobile Explorer방식, 그리고 W3C(World Wide Web Consortium)이 주도하는 i-mode방식이 경쟁하고 있다. 이러한 무선 인터넷이 제공하는 서비스의 종류는 크게 3가지로 분류할 수 있다. 첫째, 전자우편, 팩스, 통합 메시징 등의 통신 서비스가 있다. 둘째, 뉴스, 여행, 기상, 교통 정보 등 기존 음성으로 제공되던 부가정보서비스를 문자로 제공하는 문자정보서비스가 있다. 셋째, 향후 무선인터넷에서 가장 주목받는 분야로 지적할 수 있는 M-Commerce(이동전자상거래)서비스이다. E-Commerce가 인터넷의 중심이 되었듯이 무선인터넷에서는 M-Commerce가 새로운 중심이 될 것으로 예상된다. 앞으로 누구든지 언제나 어디에서든 단말기를 이용하여 손쉽게 결제할 수 있는 수단을 무선인터넷이 제공하게 될 것이며, 결국 전자상거래의 중심축도 M-Commerce로 이동할 것으로 보인다. 따라서 무

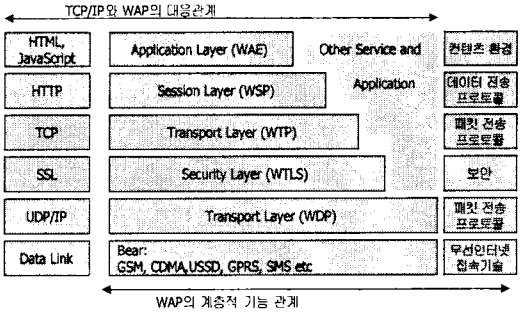
선 인터넷에서의 보안문제의 해결은 무선인터넷의 활용도를 높이는 중요 요소 중의 하나이다. 이에 본 논문에서는 무선 인터넷에서 다양한 응용 계층에 보안 서비스를 제공하기 위한 방법으로 SSL을 활용하는 방안에 대해 고찰하고자 한다. 본 논문의 2장에서는 현재 무선 인터넷의 프로토콜 및 각 프로토콜별 보안 기술에 대해 살펴보고, 3장에서는 현재 이동 단말기에서 제공되는 있는 보안 서비스를 분석한다. 그리고 4장에선 SSL의 무선 인터넷 보안 프로토콜로써 활용 방안에 대해 고찰하고, 5장에선 결론을 맺는다[2].

2. 관련연구

무선 인터넷에 대한 관심이 증가하면서 효율적으로 무선 인터넷을 사용하기 위한 무선 인터넷 프로토콜이 제시되었다. 크게 두 가지로 분류하면 WAP방식과 TCP/IP방식이 있다. WAP방식은 TCP/IP와는 독립적으로 무선 환경에 적합하게 만든 프로토콜로 WAP포럼에서 정의한 방식이며, TCP/IP방식은 유선 환경의 프로토콜을 무선 환경에 그대로 적용시킨 방식으로 Microsoft사의 ME방식과 NttDoCoMo의 i-mode 방식이 있다. 2.1절에서는 WAP프로토콜의 동작 원리와 WAP에서 제공하는 보안 기술을 살펴보고, 2.2절에서는 TCP/IP프로토콜을 이용하는 방방식 중 Microsoft사의 ME방식과 ME방식에서 제공하는 보안 기술에 대해 살펴본다.

2.1 WAP 프로토콜 및 보안기술

WAP(Wireless Application Protocol)은 이동전화나 PDA등 소형 무선 단말기 상에서 인터넷을 사용할 수 있게 하기 위해 WAP포럼이 제안한 무선 인터넷 프로토콜이다. [그림 1]은 WAP프로토콜과 TCP/IP와의 대응관계를 나타내며, 차이점을 살펴보면 다음과 같다. 즉, 데이터 전송 프로토콜은 유선의 HTTP대신 WAP에선 WSP를 사용하며, 패킷전송을 위해선 TCP와 대응되는 WTP와 WDP프로토콜을 사용한다. 그리고 보안 프로토콜로는 WTLS를 사용하며, 무선 인터넷 접속을 위해 GSM, CDMA, GPRS, SMS등을 사용한다. WAP포럼에서 정의하는 보안 프로토콜인 WTLS는 SSL/TLS에 기반하여 작성된 것으로, WAP프로토콜을 사용하는 두 응용 프로그램간의 안전한 채널을 형성하여 통신의 내용을 보장하는 방법이다. WTLS는 무결성, 기밀성 그리고 사용자 인증 서비스는 제공하지만 부인봉쇄는 제공하지 않는다. 부인봉쇄 서비스는 WAP의 응용계층에서 CryptosignText()

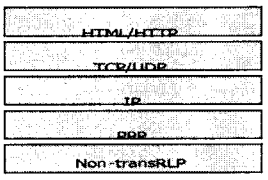


[그림 1] TCP/IP와 WAP의 대응관계

함수를 이용하여 제공한다. WTLS에서 무결성은 DES, IDEA, 3DES등의 대칭키 암호 알고리즘을 사용하여 제공하며, 무결성은 MD5, SHA등의 해쉬함수를 사용하여 제공한다. 그리고 클라이언트와 서버간의 인증은 연결 설정과정에서 가능하며, 공개키 암호화 방식과 무선 X.509인증서가 사용된다. 하지만 WTLS를 이용한 보안 솔루션은 종단간 보안(End-to-End Security)문제가 존재한다. 왜냐하면 WAP프로토콜은 무선구간에선 WTLS를 이용하여 보안 서비스를 제공하지만, 유선구간에선 SSL을 이용하여 보안 서비스를 제공하기 때문에 유·무선 프로토콜의 변환작업을 수행하는 WAP Gateway에서 평문이 노출된다. WAP을 이용한 무선 인터넷 서비스가 증권, 금융등의 전자상거래 분야에서 적용되려면, 우선 종단간 보안 문제를 해결해야 한다[3][4].

2.2 ME프로토콜 및 보안기술

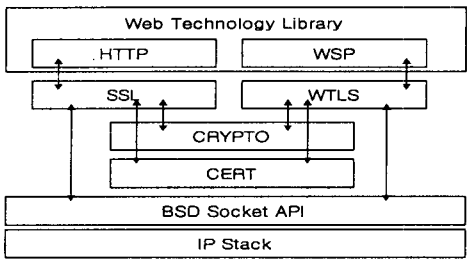
ME(Mobile Explorer)는 유선 인터넷의 TCP/IP, HTTP를 무선에서 활용하여 무선 인터넷 서비스를 제공하기 위해 Microsoft사가 제안한 방법이다. HTML의 부분집합인 m-HTML을 사용하고 Internet Explorer에 해당하는 Mobile Explorer(MME)를 단말기의 웹 브라우저로 사용한다.



[그림 2] MME Stack

[그림 2]는 MME Version1.0의 구조로, 유선 인터넷

에서 제공하는 컨텐츠를 무선에서 사용할 수 있게 만들었다. ME1.0에는 보안 서비스를 위한 보안 프로토콜인 SSL이 포함되어 있지 않으며, 향후 MME2.0에서는 SSL과 WTLS 서비스를 제공하도록 제안되었다[5].



[그림 3] MME2.0의 보안기술 구조

[그림 3]은 MME2.0에서 제시된 보안기술 구조로, TCP 소켓은 SSL, WTLS를 지원한다.

3. 단말기별 무선 인터넷 보안 서비스

현재 무선 인터넷을 사용하는 방법에는 휴대폰형 단말기를 이용하는 방법과 PDA형 단말기를 이용하는 방법이 있다. 휴대폰형 단말기를 이용하여 무선 인터넷을 사용할 경우는 WAP프로토콜을 사용하는 WAP 방식과 TCP/IP프로토콜을 이용하는 ME방식으로 분류할 수 있으며, 현재 국내에선 SKTelecom, 신세기통신, LGTelecom에서 WAP방식을 사용한다. 그리고 한국통신 엔닷컴과 한국통신 프리텔에서는 ME방식의 무선 인터넷 서비스를 제공하고 있다. 무선 인터넷을 사용하는 두 번째 방법은 PDA형 단말기를 이용하는 것이다. PDA(Personal Digital Assistant)는 과거에는 개인 정보 관리, 전자 수첩등의 용도로 사용되었지만, PDA가 무선 통신 기능과 결합하면서 무선 인터넷을 위한 이동 통신 단말기로 사용되고 있다. PDA형 단말기는 키보드의 유·무에 따라 HPC(Handheld PC)와 PPC(Palm Sized PC)로 나뉘며, OS에 따라 Palm OS형 PDA, Windows CE형 PDA, CellVic OS형 PDA로 분류된다. PDA를 이용하여 무선 인터넷을 사용하는 방법은 WAP, ME방식을 이용하는 방법과 PDA자체에 내장된 TCP/IP모듈을 이용하여 PPP통신으로 무선 인터넷을 사용하는 방법이 있다. 무선 인터넷 단말기로써 PDA의 장점은 첫째, 휴대 전화용 단말기에서보다 풍부하고 효율적인 무선 인터넷 서비스를 가능하게 한다는 것이다. 즉, 핸드폰에서 무선 인터넷을 접속하려면 별도의 페이지를 구성해야 했지만 PDA는 HTML형식의 기존의 인터넷 페이지를 볼 수 있다. 둘째, 이미지 서비스에 제약이 있는 휴대폰 형 단말기에 비해 PDA는 여러 형태의 그래픽 이미지를 제공할 수 있다. 뿐만 아니라 디스플레이에서도 휴대폰에 비해 넓은 화면에 기존 인터넷 페이지를 그대로 사용할 수 있다[6]. 그리고 넷째는 휴대폰에서 사용하는 무선 인터넷 서비스가 웹 어플리케이션에 국한되어 있는데 반해, PDA를 통한 무선 인터넷 서비스는 HTTP, FTP, TELNET등 다양한 응용계층을 위한 무선 인터넷 서비스를 제공할 수 있다. 현재 휴대폰을 이용한 무선 인터넷에서 제공되는 보안 서비스와 PDA를 이용한 무선 인터넷에서 제공되는 보안 서비스를 살펴보면 다음과 같다. 우선 휴대폰으로 무선 인터넷을 이용할 경우, WAP방식을 사용하는 이동 통신사인 SKTelecom, LGTelecom에서는 자체 보안 모듈을 개발하여 보안 서비스를 제공하고 있으며, SKTelecom은 현재 011 n-Top휴대폰에 보안 모듈을 탑재하였다. 그리고 SKTelecom이 제공하는 보안 서비스는 휴대폰에 내장된 암호화 모듈과 웹 서버 쪽에 설치된 011암호화 모듈이 직접 암·복호화를 수행한다. LGTelecom에서 제공하는 보안 서비스는 WML을 사용하는 경우만 가능하며, SKTelecom과 동일하게 클라이언트 측의 보안 모듈과 서버 측의 보안 모듈이 암·복호화를 수행한다[7]. 그리고 ME방식을 사용하는 한국통신 프리텔과 한국통신 엔닷컴은 ME1.0에서 제공하지 않는 SSL보안 서비스를 위해 국내 소프트포럼사의 SSL솔루션(MSSL)을 사용하고 있다[8]. 무선 인터넷을 PDA를 통해 이용할 경우의 보안 서비스는 3가지로 제공된다. 우선 ME방식에 적용된 보안 서비스를 사용하는 방법과 WAP프로토콜의 보안방식을 적용하는 것이다. 그리고 Pocket PDA의 경우는 Pocket Internet Explorer이 지원하는 128bit SSL에 의해 데이터의 암·복호화 기능을 수행한다[9]. 지금까지 휴대폰형 단말기를 통한 무선 인터넷 방법과 PDA형 단말기를 통한 무선 인터넷 방법에 대해 살펴보았고, 각각에 대해서 현재 제공되고 있는 보안 서비스에 대해 알아보았다. 하지만 기존에 제시되어 있는 보안 서비스의 경우 보안 서비스를 제공받는 대상은 웹 어플리케이션에 국한되어 있고, TELNET, FTP서비스, 그리고 사용자가 정의한 다양한 응용 서비스에 대해서는 보안 서비스를 제공하지 못한다. 현재 웹 서비스만 지원하는 휴대폰과는 달리 웹 이외의 응용 서비스를 제공할 수 있는 PDA에서의 보안 역시 웹 어플리케이션에 대한 보안 서비스만 제공하고 있다. 따라서 본 논문에서는 무선 인터넷에서

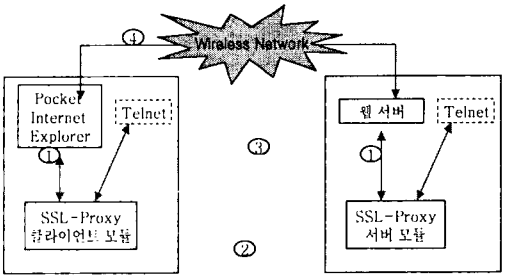
웹 서비스와 TELNET, FTP서비스, 그리고 사용자가 정의한 응용 서비스에 Securtiy를 제공하는 보안 모듈의 설계방안에 대해 고찰하고자 한다. 그리고 이는 유선에서 전송계층의 보안 프로토콜이었던 SSL을 활용하여 설계되었으며, SSL을 무선 인터넷에 활용하였을 경우 무선 인터넷 환경에 최적화 될 수 있는 암호 알고리즘에 대해서도 살펴본다.

4. 무선 인터넷에서의 SSL활용방안 제시

SSL(Secure Socket Layer)은 Netsacpe사에서 웹 보안을 위한 목적으로 개발한 보안 프로토콜이다. 인터넷의 전송계층을 위한 보안 프로토콜에 관한 연구가 활발히 진행됨에 따라 IETF(Intern Engineering Task Force)의 TLS(Transport Layer Security)Working Group에서는 인터넷 전송계층의 프로토콜로 SSL과 유사한 형태의 TLS를 표준으로 제정하였다[10][11]. SSL 및 TLS가 제공하는 Securtiy서비스는 기밀성, 무결성, 인증 기능이며, 부인봉쇄 서비스는 제공하지 않는다. 유선 인터넷의 주요 보안 프로토콜인 SSL이 무선 인터넷에서도 활용되고 있지만, 기존에 제시된 보안 서비스는 많은 문제점이 존재한다. 3절에서 살펴보았듯이 현재 제공되고 있는 대부분의 무선 인터넷 보안 모듈은 브라우저 자체에 내장되어 있어 HTTP 응용서비스만을 지원한다. 그리고 자체 내장형이 아닌 보안 모듈 역시 HTTP외의 TELNET, FTP등의 경우에는 보안 서비스를 제공받지 못하고 있다. 따라서 본 절에서는 무선 인터넷에서 다양한 응용계층을 위한 보안서비스를 제공하는 방안으로 Proxy형태의 SSL 보안 모듈을 제안한다. 그리고 무선 인터넷의 특성을 고려하여 무선 SSL-Proxy에 적당한 암호 알고리즘에 대해 고찰한다.

4.1 무선 SSL-Proxy설계

본 논문에서 제안한 Proxy형태의 보안 모듈 구성도는 [그림 4]과 같다. 우선 SSL-Proxy는 무선 단말기를 통해서 서버로 전송되는 무선 인터넷 데이터가 SSL기능 지원의 필요여부에 따라 두 가지의 전송형태를 가져야 한다. 즉, 보안 서비스(SSL)을 지원할 필요가 없는 데이터인 경우는 [그림 4]의 4번 경로로 전송이 되며, 보안 서비스를 적용해야 하는 데이터인 경우에는 1,2번 경로를 통해 SSL기능을 제공받는다. 이처럼 전송 데이터에 대한 경로를 분류한 이유는 무선 단말기의 처리속도, 용량, 이동통신 환경의 낮은 대역폭, 전송속도등 무선 인터넷 환경이 지니는 특성으로



[그림 4] SSL_Proxy 구성도

무선 인터넷의 사용시 오버헤드를 최대한 감소시키기 위해서이다. 그리고 이동 단말기의 메모리 사이즈와 데이터 처리속도를 효율적으로 이용하기 위해 SSL-Proxy는 Demon형태로 구현해야 단말기가 부담하는 오버헤드를 감소시킬 수 있다. 그리고 SSL을 브라우저에 내장형이 아닌 Proxy형태로 구현함으로써 PDA등의 무선 단말기를 통해 웹 서비스와 그 외의 다양한 응용 계층에 대한 보안 서비스가 제공될 수 있다.

4.2 무선 인터넷을 위한 SSL암호 알고리즘

SSL에서는 암호화를 위해서는 대칭키 알고리즘을 사용하고, 전자서명과 키교환을 위해서는 공개키 알고리즘을 사용한다. 그리고 무결성을 위해서는 해쉬 알고리즘을 사용한다. SSL에서 사용되는 공개키 알고리즘에는 RSA, DH-anon, Fortezza, DH/DHE-DSS/RSA, Kerberos등을 지원하고, 대칭키 알고리즘은 IDEA, RC2, RC4, DES, 3DES Fortezza등을 지원한다. 그리고 해쉬 알고리즘은 MD5와 SHA-1을 지원한다. 하지만 무선 인터넷의 데이터 전송 용량 및 전송 속도 등의 제약 사항으로 SSL의 모든 암호 알고리즘을 무선 인터넷 환경에 적용시킬 수는 없다. 따라서 본 논문에서는 공개키 알고리즘으로 가장 대표적인 RSA128bit만을 SSL_Proxy모듈에 포함시키고, 암호화 알고리즘으로는 국내 암호 알고리즘인 SEED와 RC4 128bit를 제안한다. 그리고 끝으로 무결성 검증을 위한 해쉬 알고리즘은 유선에서 사용하는 MD5와 SHA-1를 제안한다.

5. 결론 및 향후과제

무선 인터넷에 대한 관심은 1999년 이동 통신 사업자를 중심으로 시작되어 최근 IMT-2000의 등장으로 증가하고 있으며 무선 인터넷과 관련된 컨텐츠, 단말

사업, 표준화등 활발한 연구가 진행중이다. 인터넷에 대한 관심을 증대시켰던 요인 중 하나인 E-Commerce (전자상거래)는 무선 인터넷에서도 중요한 서비스의 하나로 부각되고 있지만, 무선 인터넷에서 E-Commerce가 활성화되려면 유선 인터넷 수준의 보안기능 구현되어야 한다.

따라서 본 논문에서는 현재 무선 인터넷의 주된 프로토콜인 WAP(Wireless Application Protocol)을 이용한 방식과 TCP/IP프로토콜을 이용한 ME(Mobile Explorer)방식에 대해 살펴보고, 무선 인터넷을 사용하는 이동 단말기를 중심으로 실제 제공되고 있는 보안 서비스를 살펴보았다. 그리고 이를 바탕으로 기존 무선 인터넷 보안의 문제점을 분석한 후, 무선 인터넷에서 다양한 응용 서비스를 제공하기 위한 보안 모듈을 SSL을 활용하여 제시하였다.

본 연구는 향후 실제 Windows CE기반의 Pocket PC에 구현할 것이며, SSL에 적용된 공개키 알고리즘으로 현재 무선환경에 적합한 알고리즘으로 제시된 타원곡선 알고리즘(ECC)를 탑재할 것이다.

[참고문헌]

[1] WAP기술/시장 보고서 - 한국전자통신 연구원
[2] 무선 인터넷 백서 2002 - 소프트뱅크 미디어
[3] http://www.wapforum.org
[4] Charles Arehart 외 12명 저 "Professional WAP" WROX Press
[5] 박남재, 송유진 "모바일 서비스 플랫폼 기반의 무선 전자상거래 보안 기술" 한국 정보보호학회지 11권 4호 2001.8
[6] 고재관 "Starting Mobile PDA Programming" 삼각프레스
[7] (주)애니빌 무선 인터넷연구소 "무선인터넷 개발 및 비즈니스 Guide" (주) 애니빌
[8] http://www.softforum.co.kr
[9] http://www.microsoft.com/mobile
[10] http://www.netscape.com
[11] Eric Rescorla "SSL and TLS" Addison Wesley