2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

PDA 상에서의 전자 상거래 보안 솔루션

허재형, 신동규
세종대학교 정보통신대학원
e-mail : huhjh@sktelecom.com, shindk@sejong.ac.kr

M-Commerce Security Solution for PDA

Jae-Hyung Huh, Dongkyoo Shin
Graduate School of Information and Communication, Sejong University

요 약

Handset 을 통한 m-Commerce 시장의 확장과 더불어 커머스를 기반으로 한 물류서비스, 무선 인트라넷, 모바일 증권거래 등에 PDA(Personal Digital Assistant)를 정보단말로 이용하는 서비스가 늘어나면서 PDA 무선 보안솔루션 개발에 관련된 관심이 잇따르고 있다. 특히 PDA 무선 보안솔루션은 무선 PKI 를 비롯해 암호화 솔루션, 백신, 파이어월 등 다양한 분야에서 독특한 기술이 개발되고 있으며 보안분야의 새로운 시장을 형성할 것으로 기대된다. PDA 무선 보안 솔루션은 증권, 뱅킹 등에서 시도 되어지고 있는 Application layer 에서 암호/복호화 하는 방식, 유선과 동일하게 브라우저/ 웹서버에서 제공하는 SSL 암호화 방식, SSL v3 및 TLS v1 과 호환되는 자체 암호화 모듈 방식등의 3 가지로 크게 나누어 볼수 있다.본 논문에서는 WinCE OS 의 iPaq PDA 에 SSL v3 및 TLS v1 과 호환되는 자체 암호화 모듈 방식의 시스템을 설계한다. PDA 와 서버 간의 인증, 메시지 기밀성 및 무결성을 충족시킬 수 있는 보안 서비스를 제공하고 유선과 동일한 수준의 보안 수준을 유지하면서도 지금까지 무선 암호인증의 문제점이었던 소용량 무선단말기의 한계를 극복하는 PDA 용 무선 보안 솔루션을 설계하는데 목적을 두고 있다.

1. 서론

국내의 무선인터넷 시장은 다수의 음성전화 가입자를 보유한 이동통신사업자를 중심으로 전개되고 있으며 향후 CDMA 2000-1x 등의 IMT-2000 서비스가 활성화되어 패킷 방식의 무선데이터 서비스가 보편화되면 통신요금에 대한 사용자의 부담은 줄어들 것으로 보이며, 이동단말기(Smart Phone, PDA) 및 보안, 지불 등의 무선인터넷 관련 솔루션의 발달로 기존의 유선 인터넷과 유사한 수준의 서비스를 제공할 수 있을 것이다. 결국, 무선인터넷은 우리의 삶의 일부인 보편적인 서비스가 될 것으로 보인다.

치열하게 경쟁하고 있는 Handset 의 경우 WAP(Wireless Application Protocol) 진영과 ME(Mobile Explorer) 진영으로 나누어져 있고 각각 WPKI(Wireless Public Key Infrastructure)기반의 전자 상거래 솔루션을 발빠르게 준비하고 있다. 이에 비해 PDA 경우 아직 m-Commerce 단계 이전에 기본 컨텐트를 제공하는 수준이다. 보안 수준 역시 증권, 은행사 서비스 등에 개별적인 Application Level 의 E2E(End-to-End) 보안 솔루션이 구축되어져 있을 뿐 Handset 과 같은 WPKI 를 고려한 보안 솔루션은 미약한 면이 많다.

PDA 무선 보안 솔루션은 증권, 뱅킹 등에서 시도되어지고 있는 응용계층(Application layer)에서 암호/복호화 하는 방식, 유선과 동일하게 브라우저, 웹서버에서 제공하는 SSL 암호화 방식, SSL v3 및 TLS v1 과 호환되는 자체 암호화 모듈 방식등의 3 가지로 크게 나누어 볼 수 있다. 또한 유선 PC 의 http 프로토콜을 대부분 사용한다는 유선적인 측면과 PDA 단말기 자체가 시스템 리소스가 열악하고 네트워크이 무선이라는 무선적인 측면으로 유선, 무선에 중간적인 성격을 가지고 있다고 볼 수 있다. PDA 용 무선 보안 솔루션은 유선적인 측면과 무선적인 측면이 모두 고려 되어 설계 되어야만 한다.

본 논문은 무선인터넷 분야로의 사업영역 확대 및 시장 선점을 위해 PDA 상에서의 전자 상거래와 보안 솔루션을 설계하는데 목적을 두고 있다. 본 논문의 구성은 다음과 같다. 보안 모듈중 응용계층에서 암호

/복호화 하는 방식, 유선과 동일하게 브라우저와 웹 서버에서 제공하는 SSL 암호화 방식을 설명하고, 본 논문에서 제시하는 WinCE OS 의 iPaq PDA 에 SSL v3 및 TLS v1 과 호환되는 자체 암호화 모듈 방식의 시스템을 설명한다.

2. 관련 연구

2.1 유선과 동일한 SSL 암호화 방식

일반적으로 유선 PC 에서 많이 사용하는 이 암호화 방식의 장점은 사용자가 특별한 프로그램을 다운로드 받지 않아도 일반적으로 많이 사용하는 넷스케이프와 익스플로러가 자동으로 보안 채널을 맺어주는데 있다.

일반 http 요청인 경우에는 암호화 모듈이 작동 되지 않고 특정 https 요청인 경우 MS 의 Internet Explore 같은 브라우저에 포함되어 있는 암호화 모듈이 웹서버에 포함되어 있는 암호화 모듈과 연동하여 SSL 채널을 생성하고 데이터를 암호화하게 된다.[1]

단점으로는 브라우저에서 인식되어있는 인증기관에서 발급 받은 서버 인증서인 경우만 에러, 경고 메시지 없이 작동하게 된다.

무선인 경우 속도가 느리고 증권등에서 필수적으로 사용하는 SEED 알고리즘을 지원하지 않는다.

2.2 Application Layer 에서 암호화 방식

이 암호화 방식은 SSL 등의 채널을 사용하지 않고 Application 간에 암호화 모듈을 연결하여 사용하는 방식이다. 주로 증권,뱅킹등에서 주로 사용하는 방식이다.

Html 페이지 상에서 Active x 컨트롤등을 다운 받게 하고 보안 서비스인 경우 Active x 컨트롤을 구동하여 데이터를 암호화 하고 전송한다. 물론 서버쪽에서도 Actvie x 컨트롤과 연동할수 있는 암호화 모듈이 개발 되어져야 한다.

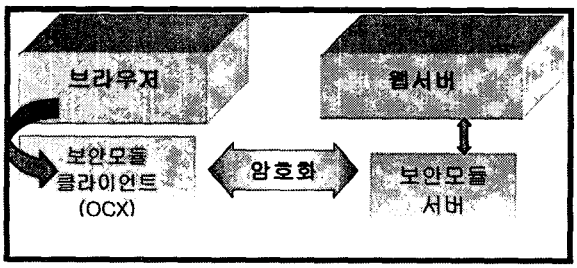

그림 1 Application Layer 에서 암호화 방식

3. SSL v3 및 TLS v1 과 호환되는 자체 암호화 솔루션의 시스템 설계

3.1 시스템 개요

본 논문에서는 PocketPC 인 iPaq 만을 고려하여 설계를 진행하였으며 SSL v3 및 TLS v1 과 호환되는 자체 암호화 방식을 간단히 " PDA-TLS" 라고 명명하였다.

PDA-TLS 를 사용하여 PDA 와 서버 간의 인증, 메시지 기밀성 및 무결성을 충족시킬 수 있는 보안 서비스를 통해 PDA 기반 무선인터넷 환경에서 보안 응용서비스에 대한 End To End 보안, 서버 인증, 메시지 무결성 서비스 등을 제공을 하는데 본 시스템은 목적을 두고 있다.

PDA-TLS 가 제공하려는 서비스는 아래표와 같다.

서비스명	내 용
SSL 및 TLS 암호화 서비스	인증서버로부터 발급 받은 서비스 서버용 서버 인증서를 통해서 서비스 서버를 인증하고 다양한 응용 프로그램으로부터의 보안 요청을 처리하기 위한 보안 서비스
ECC 암호 서비스	PDA 또는 Mobile Phone 과 같이 리소스가 극히 제한적인 환경에서 아주 적은 리소스만을 사용하는 ECC 암호 시스템을 지원함으로써 보안 응용

표 1. 서비스 내용

표 1 과 같이 PDA-TLS 는 기존 PDA 에서 제공하는 TLS(SSL) 통신 서비스 확장과 제한된 PDA 에 최적화된 보안/인증 알고리즘 구현,각 응용에서 요구하는 충분한 보안/인증 레벨 제공을 필수로 한다.

3.2 시스템 기능

3.2 1 SSL v3 및 TLS v1 기능

전송계층 보안 프로토콜의 주요한 목적은 두 어플리케이션 간의 통신 시 요구되는 보안과 인증 서비스를 어플리케이션에 Transparent 하게 제공하는 것이다. 전송계층 보안 프로토콜은 두 레벨로 구성되어 있다. 하위레벨은 신뢰할 수 있는 전송 프로토콜(e.g., TCP[TCP]) 위에 위치하며 Record Protocol.이라 한다. Record 프로토콜은 다양한 상위레벨 프로토콜들을 캡슐화하는 기능을 제공한다. 상위레벨인 Handshake Protocol 은 서버와 클라이언트간의 인증을 가능하게 하며, 또한 어플리케이션 프로토콜이 전송되거나 수신되기 전에 이루어지는 암호화 알고리즘, 암호 키에 관한 협상을 가능하게 한다.[2]

본 시스템은 전송계층 보안 프로토콜인 SSL v3 와 TLS v1 표준과 호환성을 제공하여야만 한다.

3.2.2 암호 슈트 (Crypto Suite) 확장 기능

제한된 무선환경에서 최적화된 보안/인증 서비스 지원 및 국내 표준을 만족하기 위해 다음의 확장 보안 알고리즘 슈트를 지원한다. 단, ECC(ECDH) 타원곡선은 일반적인 WPKI 기존 무선용 인증서와의 호환성을 고려하여 WTLS 3,5 번 곡선만을 지원하기로 한다.

확장 내용

SEED 128 CBC - RSA 1024 - SHA 1
3DES EDE CBC - RSA 1024 - SHA 1
SEED 128 CBC - ECDH(Curve 3,5) - SHA 1
3DES EDE CBC - ECDH(Curve 3,5) - SHA 1

표 2. 암호 슈트 (Crypto Suite) 확장 내용

3.2.3 ECDSA (Elliptic Curve Digital Signature Algorithm) 전자 서명 인증서 처리 기능

PDA 와 같이 리소스가 제한적인 환경에서는 작은 키 사이즈로 높은 안정성을 보장하는 ECC 서명 알고리즘이 유리하다. 무선용 X.509 v3 ECDSA 전자 서명 인증서를 사용하여 TLS 프로토콜을 구현한다.[3]

3.3 시스템 구성

3.3.1 시스템 개념도

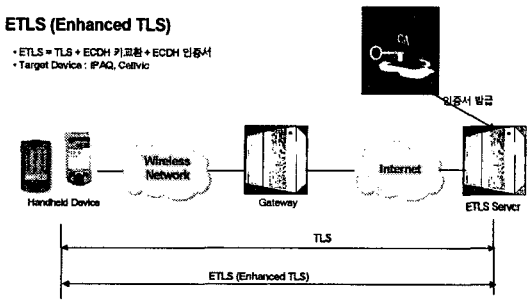

그림 2 PDA-TLS 시스템 구성도

PDA-TLS 는 기존 SSL v3 및 TLS v1 프로토콜을 준수하면서, 추가로 ECDSA 서명 인증서를 기반으로 하는 ECDH Handshake 가 가능하도록 확장하였는데 이러한 모듈은 특히 PDA 와 같이 리소스가 극히 제한적인 환경에 적합하다.

그림 2 에서 언급되어진 ETLS(Enhanced TLS)는 PDA-TLS 가 제공해주는 확장된 기능으로 ECDH 키교환과 ECDH 인증서를 통하여 TLS 프로토콜로 암호화 하는 방식을 의미한다. ETLS 서버는 ETLS 를 지원해 주는 서버 보안모듈이다.

PDA-TLS 보안시스템은 PDA 와 서비스 서버 간에 TLS(SSL) 프로토콜을 통해서 안전한 채널을 구성함으로써 증권/무선뱅킹 등 사용자 인증, 기밀성 등의 보안기능이 필요한 서비스를 가능하도록 한다.

사용자는 PDA-TLS 시스템이 탑재된 PDA 를 사용해서 해당 서비스 서버의 URL 만 입력하면 PDA-TLS 시스템이 어플리케이션 데이터들을 안전하게 서비스 서버로 전송하게 된다. ETLS 서버는 이러한 과정에서 기존의 공인 또는 사설 인증서버를 통해서 발급받은 무선용 인증서를 통해서 신뢰성을 입증하게 된다.

3.3.2 시스템 동작

iPAQ 과 CellVic 등 단말기별로 PDA-TLS 모듈을 호출하는 과정은 조금 다르지만, 호출된 이후의 동작과정은 같으며 SSL(TLS) 프로토콜을 이용하게 된다. 일반적으로 SSL(TLS) 프로토콜은 두 레벨로 구성되어 있다. 하위레벨은 신뢰할 수 있는 전송 프로토콜 (e.g., TCP[TCP]) 위에 위치하며 Record Protocol 이라 한다. Record 프로토콜은 다양한 상위레벨 프로토콜들을 캡슐화하는 기능을 제공한다. 상위레벨인 Handshake Protocol 은 서버와 클라이언트간의 인증을 가능하게 하며, 또한 어플리케이션 프로토콜이 전송되거나 수신되기 전에 이루어지는 암호화 알고리즘, 암호 키에 관한 협상을 가능하게 한다.[4] SSL(TLS)의 잇점중의 하나는 어플리케이션 프로토콜과 독립적이다라는 것이다. 상위레벨 프로토콜은 SSL(TLS) 프로토콜 위에서 투명하게 전송되어질 수 있다.

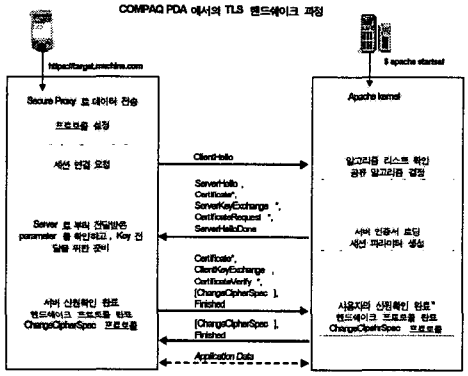

그림 3 PDA-TLS 핸드세이크 과정

PDA-TLS 의 동작 프로세스는 아래와 같다.

1) 브라우저에서 사용자가 접속을 원하는 URL 을 입력

2) 브라우저는 40bit SSL 로 PDA-TLS 와 접속

3) PDA-TLS 는 128bit SSL 로 웹서버에 접속

4) 브라우저에서 보내오는 40bit 로 암호화된 데이터를 PDA-TLS 가 128bit 암호화 된 데이터로 변환하여 전송

5) 서버에서 보내오는 128bit 로 암호화된 데이터를 PDA-TLS 가 40bit 암호화 된 데이터로 변환하여 브라우저로 전송[5]

PDA-TLS 는 클라이언트단에서는 Security Proxy 로서 동작한다. 즉 브라우저에서 서버로의 연결은 항상 두가지의 SSL 접속이 이루어지게 된다.

첫번째는 브라우저와 PDA-TLS 사이에서의 접속으로 브라우저가 클라이언트로 PDA-TLS 는 서버로서 동작하여 SSL 접속을 한다. 이때 브라우저는 40bit SSL 만을 지원하기 때문에 이 구간의 SSL 접속은 40bits SSL 접속만이 이루어진다. 이 40bit SSL 접속은 로컬 PC 환경에서 이루어 지므로 40bit 암호화에 대한 위험성

은 없다고 볼 수 있다. 혹자는 로칼환경의 40bits SSL 을 같은 LAN 에 묶여 있는 다른 시스템에서 스니핑을 해서 풀수 있다고 하지만 실제 TCP/IP 스택은 로칼(127.0.0.1)주소로 보내는 패킷은 로컬 시스템 밖으로 내보내지 않으므로 스니핑이 불가능하다.

두번째는 PDA-TLS 와 웹서버와의 접속으로 PDA-TLS 의 SSL-128 모듈은 클라이언트로 웹서버는 서버로서 동작하여 SSL 접속을 한다. 이때에는 PDA-TLS 가 128bit SSL 을 지원함으로 128bit SSL 접속이 이루어진다.

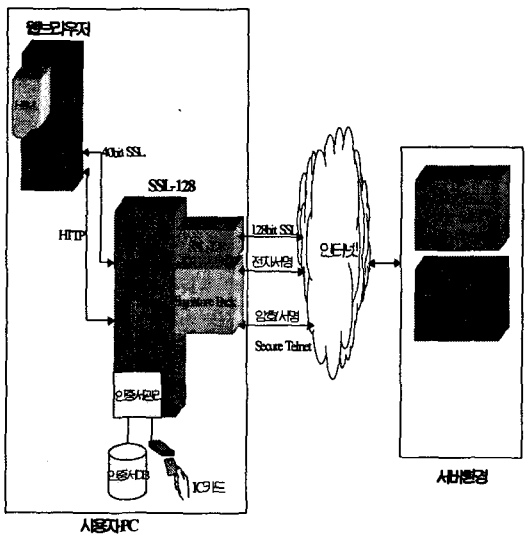

그림 4 PDA-TLS 시스템 구조

SSL-128 모듈은 웹브라우저의 Security Proxy 를 통해 40bits SSL 트랜젝션을 받아 128bits SSL 트랜젝션으로 변환해 128bits SSL 웹서버와 통신을 하는 모듈. 주고 받는 모든 정보를 모두 암호화 한다. 이 모듈을 이용할 경우에는 웹서버가 반드시 128bits 표준 SSL 을 지원해야 하므로 사용하고자 하는 웹서버가 128bits SSL 을 지원하지 않을 경우에는 128bits SSL 을 지원하는 웹서버를 게이트웨이로 앞단에 설치하는 형식으로 지원한다.

Signature Pack 모듈은 웹브라우저에서 웹서버로 전송되는 데이터를 사용자의 전자인증서를 이용해 전자서명하여 서버에게 전달한다. Signature Pack 은 HTTP 를 통해서 전송되는 데이터도 서명을 할 수 있으며, HTTPS(SSL 암호화 전송)를 통해 전송되는 데이터도 서명을 할 수 있다. Signature Pack 의 장점은 하나의 모듈이 두종류의 브라우져 즉 넷스케이프와 익스플로러를 구분없이 하나의 프로그램으로 하나의 인증서를 이용해 지원한다.[6]

3.3.3 시스템 고려 사항

기존 브라우저에서 40bit SSL 접속이 PDA-TLS 를 사용함으로써 두번의 SSL 접속때문에 세번 암/복호화를 하므로 성능저하가 있다고 생각할 수 있으나 성능저하는 거의 없다. 이 사실은 CPU 속도와 네트워크 통신속도 비교를 통한 계산으로도 확인할 수 있으며 속도비교 테스트를 통하여 확인할 수 있었다. SSL 프로토콜은 초기 세션키를 셋업한 후에는 대칭키 암호알고리즘을 이용해 데이터를 암/복호화해 전송/수신한다. 그런데 일반적으로 팬티엄 100MHz 정도의 PC 환경에서 대칭키 암호가 초당 1.5Mbyte 정도를 암호화 한다. 그러므로 일반적으로 LAN 환경도 10Mbps(초당 1.16Mbyte, 실제로는 1/3 정도의 속도를 지원), 모뎀환경도 56Kbps(7Kbyte)정도 밖에 전송하지 못하므로 암 복호의 속도는 통신속도에 비해 월등히 빨라 속도저하에 주된 요인으로는 기여하지 못한다

4. 결론 및 향후 방향

현재 무선 인터넷에서 m-Commerce 시장이 점점 확대 되어 지고 있고 작은 화면으로 인해 한계성을 갖고 있는 Handset 의 영역을 PC 와 Handset 의 중간 영역에 있는 PDA 가 보완하리라는 기대는 커지고 있다.

본 논문에서 구현해 본 PDA-TLS 를 사용하게 될 경우 증권 서비스등에 필수적인 SEED 알고리즘을 추가할 수 있고 PDA 와 같이 리소스가 제한적인 무선 환경에서 작은 키 사이즈로 높은 안정성을 보장하는 ECC 서명 알고리즘을 사용할 수 있다.

향후 자체 WPKI 규격과도 호환을 할 수 있도록 구성할 수 있으며 CP(content provider)에게 어떤 불필요한 작업 없이 사용자에게 컨텐트를 제공할 수 있다.

현재는 iPaq 클라이언트와 아파치 웹서버만을 고려한 시스템을 설계하였지만 계속적으로 늘어나는 셀빅, Palm, 리눅스등 다양한 OS 를 가지는 단말기를 지원하여야 하며 아파치 웹서버가 아닌 다른 서버에 적용할 수 있는 서버 모듈을 구현하는 것이 큰 과제로 남아 있다.

참고문헌

[1] SET and SSL: electronic payments on the Internet Sherif, M.H.; Serhrouchni, A.; Gaid, A.Y.; Farazmandnia, F. Computers and Communications, 1998. ISCC '98. Proceedings. Third IEEE Symposium on , 1998 Page(s): 350 - 358

[2] 이병도 역, 인터넷 보안, 비앤씨, 1996

[3] 김철, 암호학의 이해, 영풍문고, 1996.

[4] 박정수, 조은경, 강신각, 박성열, " 인터넷 웹 보안 프로토콜 기능 분석," 통신정보보호학회지, 제6권, 제2호, pp. 53-76, 1996. 6.

[5] [SSL v3] " Secure Sockets Layer Version 3" , [TLS v1] " The TLS Protocol Version 1" , January 1999, IETF rfc 2246

[6] CCIB, Common Criteria for Information Technology Security Part 1 : Introduction and general model, May, 1998.