무선 인터넷 보안 연구

이직수*, 이성현*, 이재광*
*한남대학교 컴퓨터공학과
e-mail:jslee@netwk.hannam..ac.kr

A Study on Wireless Internet Security

Jik-Su Lee*, Seoung-Hyun Lee*, Jae-Kwang Lee*
*Department of Computer Engineering Hannam University

요 약

이미 유선 상의 모든 서비스가 무선 환경으로 확장되어 소비자의 요구를 충족시켜주고 있다. 전자상거래를 비롯한 각종의 데이터 서비스들은 이동통신 사업체를 중심으로 많은 서비스를 제공하고 있다. 그러나 무선 인터넷 환경에서는 하드웨어적인 제약사항 및 배터리 문제, 대역폭의 이유로 유선상의 보안 서비스를 제공하지 못하고 있는 실정이다. 낮은 연산 속도, 작은 메모리는 유선상의 큰 키 길이를 만족할 수 없고, 또한 만족하더라도 연산하는데 많은 시간이 걸리는 단점이 있다. 이와 같은 문제는 계속해서 높아지는 하드웨어 및 배터리의 성능으로 보완되고 있지만, 전자상거래 및 금융 거래와 같은 서비스에서 요구하는 보안 서비스를 만족하기에는 아직까지 역부족이다. 본고에서는 적은 사양에서 최대의 보안 서비스를 제공하기 위해서 전세계적으로 무선 인터넷 프로토콜 표준인 WAP(Wireless Application Protocol)과 무선 공개키 기반 구조(WPKI)를 살펴보고, 무선 상의 단점을 보완하도록 제시된 응용 계층 전자 서명, 암복호화 함수에 대하여 논의한다.

1. 서론[1)]

최근 무선 인터넷 서비스는 모바일 단말기를 통해서 시간과 장소를 가리지 않고 제공되어지고 있다. 더욱이 이런 모바일 단말기를 통해서 TV를 시청하고, MP3를 들으며, 인터넷 뱅킹과 게임도 할 수 있는 만능 기기로 변해가고 있다. 불과 무선 단말기가 보급되기 시작한지 십여년 사이의 놀랄만한 발전이라 하겠다. 계속해서 광범위한 서비스를 개발 중에 있으며, 그 가속화는 더욱더 빨라지고 있다. 그러나 이러한 다양한 서비스를 제공하는 무선통신 환경은 유선의 단말기와는 엄연히 성능 면에서 제약사항을 갖고 있다. 전자상거래를 비롯하여 금융 서비스의 경우 강력한 보안 서비스를 현재 제공하지 못하고 있다. 다시 말해서 다양한 서비스에는 반드시 정보보호 문제가 반드시 선결되어야 한다. 사용자의 신원을 확인하고, 정당한 사용자에 대해서는 질 좋은 서비스를 제공하고, 다른 악성 사용자들에게 비밀화 될 수 있도록 하는 보안 서비스를 본 논문에서 다루고자 한다. 먼저 전세계적으로 표준인 WAP(Wireless Application Protocol)을 살펴보고, 무선 보안 서비스를 제공하는데 그 기반이라 할 수 있는 WPKI (Wireless Public Key Infrastructure)를 논의하고, 현재 무선 보안의 문제점인 End-to-End 보안을 위해 제시된 응용 계층 보안을 논의한다.

1) 본 연구는 산업자원부에서 시행한 산업기술개발사업 (2003-61-10009504)에 의해 지원되었음

2. 무선 인터넷

무선 인터넷이라 함은 이동전화나 휴대용 단말기로 Anytime, Anywhere 인터넷에 접속하여 서비스를 제공받을 수 있는 것을 말한다. 무선인터넷 기술의 핵심은 휴대용 단말기의 한정된 자원을 감안하고 무선망과 유선망의 효율적인 결합이라고 말할 수 있다. CDMA/GSM 기반의 무선망과 TCP/IP를 사용하는 유선망을 효율적으로 연동하여, 무선단말기로부터 무선망을 통해 유선망에 위치한 컨텐츠에 효율적으로 접근할 수 있는 통신 프로토콜을 정의하는 것이 무선인터넷 기술이다. 이러한 무선 인터넷 프로토콜 표준은 크게 3가지가 있으며, Microsoft사의

MME, 일본 DoCoMo사의 i-mode, 그리고 WAP-Forum의 WAP이 있다. 무선 인터넷 프로토콜 중 1997년 6월 Ericsson, Nokia, Motolora 및 Phone.com 등 4개사를 중심으로 WAP(Wireless Application Protocol) Forum을 결성하여 무선인터넷 표준을 제정한 WAP이 전세계적으로 가장 주목받고 있으며, 계속해서 표준 제정을 위한 활동을 벌이고 있고, 현재 무선인터넷 서비스 호환을 위한 업계의 대표적인 표준으로 자리잡고 있다.

2.1 무선 인터넷 프로토콜

무선 인터넷 표준 WAP 구조는 세 개의 구성 요소 즉, 클라이언트, 서버, 그리고 이 둘 사이에서 중계 역할을 하는 게이트웨이가 있다(그림1).

그림 1 WAP 구조[1]

WAP 구조에서 핵심요소라 할 수 있는 게이트웨이는 유선의 HTTP를 무선 프로토콜로, 또는 그 반대로 변환하는 기능을 갖는다. 무선 인터넷 프로토콜 WAP의 구조는 (그림2)와 같이 5개의 다른 기능을 갖는 계층으로 되어있다. 먼저 WDP는 유선의 UDP와 유사한 비신뢰적인 데이터그램 서비스 계층을 맡고 있으며, WTLS는 무결성, 기밀성, 부인 봉쇄 서비스를 제공하는 보안 계층이며, WTP는 브라우징을 위한 요구 및 응답 형식을 지원하는 Transaction

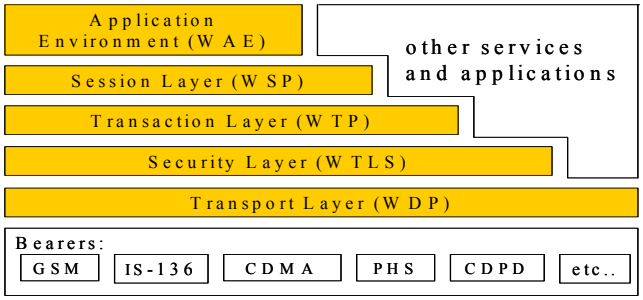

그림 2 WAP 프로토콜 구조

서비스 계층이다. WSP는 HTTP/1.1에 상응하는 기능의 계층이며, WAE는 무선 인터넷 서비스와 이동전화 서비스를 지원하는 계층이다.

2.2 WAP 정보보안 요소

앞에서도 언급했듯이 무선 인터넷에서 전자상거래를 비롯한 각종 서비스가 안전하게 이루어지기 위해서는 정보보호 문제가 반드시 밑바탕 되어야 한다. 정보보호 기술은 기존의 인터넷에서도 가장 중요한 요소로 많은 연구가 이루어지고 있으며, 특히 전자상거래와 같이 개인정보나 경제적인 정보와 관련된 서비스에서의 보안은 더욱 그렇다. 정보호호 서비스를 책임지고 있는 계층은 WTLS이다. 물론 이를 위해서 공개키 분배 및 인증에 관한 기반 구조가 필요하게 되는데 이를 위해 무선 공개키 기반 구조(WPKI)를 전제로 하고 있다. 본 논문에서는 정보보호 기술에 관련된 무선인터넷 프로토콜(WAP2.0)에서 WTLS에 적용할 수 있는 살펴본다 또 WPKI에서 요구하는 사항도 살펴보겠다. 따라서 공개키 교환과 WTLS에서 메시지 교환 형식을 살펴본다 먼저 WAP 2.0에서는 End-to-End 보안을 위한 스펙이 제시되었는데, 무선에 맞는 TCP와 HTTP를 제공하는 WAP HTTP Proxy를 새롭게 추가하고 있다(그림2). 또한 TLS 터널링 구조의 종단간 보안 형태도 제시하였는데, 구조는 (그림3)과 같다. 이는 유선과 같은 종단간 보안 제공을 제시하고 있다.

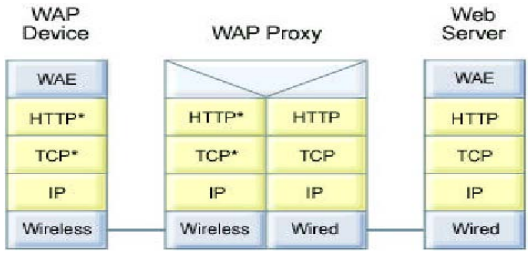

그림 3 TCP, HTTP를 사용하는 구조

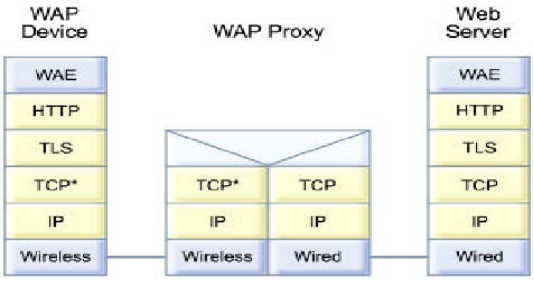

그림 4 TLS 터널링을 사용하는 구조

WTLS는 유선의 SSL의 구조와 유사하다. 데이터그램 프로토콜 WDP 상위 계층에서 작동하고 있으며, hello 메시지를 통하여 암호화 통신을 위한 세션키 재료를 주고받고, 레코드 프로토콜은 실제 데이터 암호화를 통해 기밀성과 MAC 값을 사용하여 무결성을 제공한다. 또한 WMLScript Crypto Library를 통하여 응용 계층에서의 전자서명 기능을 하는 signText함수[WAP2.0 Spec]를 통하여 부인봉쇄 서비스를 제공한다. 또한 WIM(WAP Identity Module)을 통하여 제한된 단말기 상에서 저장 공간을 보완하고 있는데, 스마트카드로 구현된 WIM에 비밀키와 인증서를 저장하게 된다. 또한 WTLS에서 이용되는 공개키를 효과적으로 관리하기 위해 IETF의

PKIX WG의 X.509를 기반으로 한 WPKI(Wireless Public Key Infrastructure)를 개발 중이다. 무선상에서 PKI 구현에 중요 고려사항을 살펴보면 무엇보다도 가장 기본이 되는 인증서 검증이다. 이는 큰 컴퓨팅 능력을 필요로 하기 때문에 현재의 무선 단말기에는 부담이 되고 이를 해결하기 위하여 WAP 모델에서는 인증서의 유효기간을 짧게하여 인증서 검증의 부하를 줄인 Shot Lived Certificate(SLC)와 써드파티를 통한 인증서 확인 방법 Online Certificate Status Protocol(OCSP)가 있다.

3 WPKI(Wireless Public Key Infrastructure)

3.1 무선 PKI 고려사항

유선과 같은 기밀성, 무결성, 인증, 부인봉쇄를 제공하기 위하여, 무선 PKI에서는 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소로 변화시켜 사용해야만 한다. 무선 PKI를 구축하는 경우에 클라이언트와 서버간의 대역폭, 클라이언트의 컴퓨팅 능력, 제한된 메모리 마지막으로 인증서 검증 메커니즘의 경량화 등을 고려해야 한다. 요약하자면 다음과 같다.

- 단말기의 메모리 제약을 고려하여 인증기간과 상호연동 할 수 있는 인증서 요청, 관리 프로토콜을 적용
- 인증서 발급, 처리, 저장, 검증 등에 필요한 프로토콜을 무선에 적합하도록 모듈 크기를 줄이고 처리 시간 감소화
- 무선인터넷 환경에 적합한 인증서 검증방식을 채택하여 단말기 컴퓨팅 능력으로 검증할 수 있게 함
- 인증서, CRL(Certificate Revocation List) 프로파일 규격을 정하여 무선에 최적화 함
- 무선 단말기 상에서 실행할 수 있도록 서명, 검증, 암호화 알고리즘을 변경, 최적화 함

3.2 무선 PKI

이동 통신 장비가 보급화 되면서 무선 인터넷은 이동성과 편리성을 내세워 엄청난 속도로 발전하고 있지만, 정보보호 서비스는 그에 발맞춰 발전하지 못하고 있다. 따라서 유선과 같은 보안 서비스 즉, 기밀성, 무결성, 인증, 부인방지 등을 제공하면서 무선에 적합할 수 있도록 변화를 요구하고 있다. 새롭게 등장한 인증서 검증 방식, 보안 모듈로써 자바카드 사용, 단대단 보안을 위한 응용계층 전자서명 및 암복호화 함수 사용 등을 예로 들 수 있다. 본고에서는 WAP을 기반으로 하는 무선 PKI를 논할 것이며, 먼저 무선 PKI의 구성요소부터 살펴보도록 한다. 무선 PKI의 구성 요소에는 크게 인증서를 발

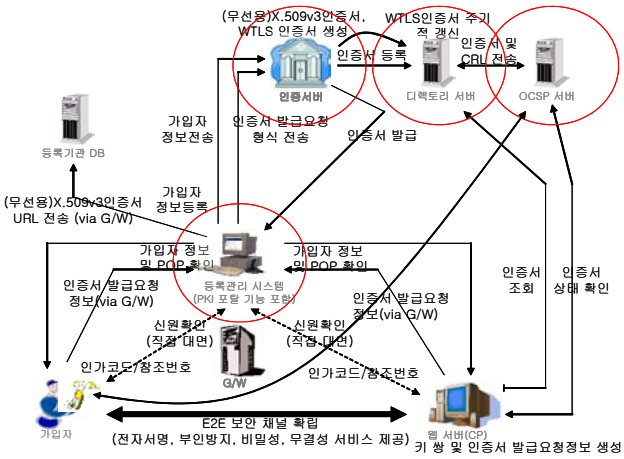

그림 5 WPKI 구조

급하고 인증서의 효력정지 및 폐지 기능을 하는 인증기관, 인증 기관과 사용자 사이에서 인증서 등록이나 신원을 확인하는 등록 기관, 인증서나 CRL을 저장하는 DataBase 그리고 사용자로 나눌 수 있다. 현재 WPKI 구조는 유선의 형태와 비슷하나, 이동통신 단말기의 제약사항으로 인해 자바카드 사용과, 인증서 검증의 부하를 줄이기 위한 OCSP를 사용함으로써 통신하는 양측 간에 인증을 통하여 안전한 통신을 제공한다. End-to-End 보안의 개념은 WALS(Wireless Application Layer Security) 전자서명 함수 및 암복호화 함수를 사용함으로 제시하고 있고, 또 안전한 통신을 위해 보안 모듈(WIM)을 사용하고 있다. WAP에서 전송계층 보안을 담당하는 WTLS에서 사용하는 난수는 Hello 메시지 교환에 사용되고 양측의 실제 통신하는 암호 알고리즘 키 재료로도 사용된다. 제한된 자원에서 WIM을 기반으로 각종 암복호화 함수 및 서명 함수를 사용하고 있다.

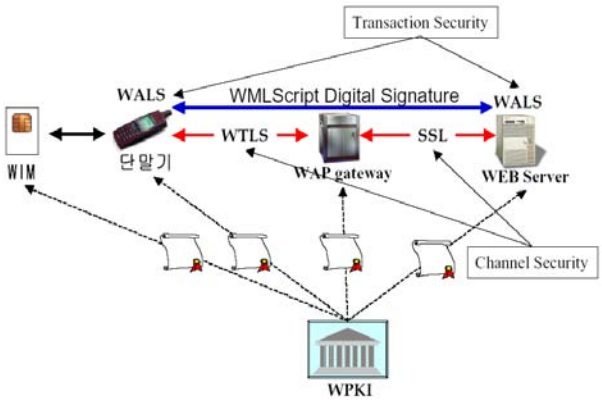

그림 6 WAP 구조

전송 계층과 WIM(Wireless Identity Module)을 사

용하여 기밀성 및 무결성 서비스를 제공하고, 응용계층의 signText 함수와 Encrypt/ Decrypt 함수를 사용하여 부인 봉쇄를 제공함으로써 결론적으로 종단간 보안을 제공하고 있다. 기존에 WAP 기반의 보안상 허점인 유무선 프로토콜 변환 시에 평문이 노출되는 위험요소를 해결하고 응용계층 보안 채널을 생성한다.

4 결론

무선 인터넷 사용자가 해마다 폭발하듯이 늘어나고, 다양한 서비스의 수요에 발맞춰 정보보호 서비스를 충족하기 위한 정보보호 시스템 개발도 함께 진행되어야한다. 무선 환경에서의 인터넷 서비스는 앞서 살펴보았듯이 유선과는 그 구조가 다르다. 모바일 단말기가 갖는 제약 사항 즉, 낮은 CPU 처리 능력, 제한된 메모리, 낮은 대역폭, 배터리 시간문제 등이 유선과 동급의 정보보호 서비스 제공을 가로막고 있다. 계속해서 단말기의 사양은 발전하여 현재 단말기가 갖는 많은 제약사항들은 곧 사라질 것으로 예상된다. 본 논문에서는 단말기 제약 사항을 극복하기 위한 WAP 기반의 트랜잭션 보안을 위해서 무선 PKI에 WIM을 사용하여 인증서 검증 부하를 줄이고, 부인 봉쇄 서비스를 위해 응용 계층에서 전자서명 기능을 제공하며 WAP 2.0 Security Spec 표준 문서의 암호화 함수를 구현하여 보다 안전한 종단간 보안을 제공하도록 해야한다. 현재 WAP 2.0 Security Spec 문서에서는 전자서명 함수와 암호화 함수를 제안해 놓은 상태이고, 그 밖에 WAPForum의 Working Group에서 WPKI를 경량화 시킬 수 있는 함수나 기능을 개발 중에 있으며, 각 이동통신 개발자들로 하여금 직접적인 참여를 권하고 있다. 각 이동통신사마다 따로 개발하는 불합리한 국내 상황을 하나의 플랫폼에서 개발할 수 있도록 하고 있으며 이는 무선 인터넷 보안 시스템 개발에 원동력으로 제공 될 것으로 보인다.

참고문헌

[1] certicom, Complete WAP Security

[2] 김준길, “전자상거래의 개념과 발전방향”, 정보과학회지, 제 16권 제 5호, 5. 1998

[3] 김현욱외4명, “Wireless Application Protocol 서비스 개요”, SK Telecom Technical Journal. Vol6 No 4, 10, 1999

[4] WAP Forum, "Wireless Application Protocol Wireless Transport Layer Security Specification version18-FEB-2000", feb, 2000

[5] The SSL Protocol version 3.0, Netscape Communications Corp. Mar, 1996

[6] 배석희, “모바일 플랫폼 표준화 동향 및 향후 발전 방향”, TTA 저널, 제 82호, 2002, 7, 8. 20p

[7] 무선공개키 기반구조 표준, WAP-217-WPKI-20010424-a

[8] ISTF-022 무선응용계층 보안프로토콜 표준

[9] IETF RFC 2560(1996.3), Internet X.509 Public Key Infrastructure Certificate Management Protocols