WAP 기반의 Application Layer 암호화 기법 분석

황영철* · 최병선* · 이성현* · 이원구* · 이재광*
한남대학교 컴퓨터공학과

Analysis of Cryptography Technique on Application Layer based on WAP

Young-Chul Hwang, Byung-Son Choi, Sung-Hyun Lee, Won-gu Lee, Jae-Kwang Lee
*Dept of Computer Engineering, Hannam University
E-mail : ychwang@netwk.hannam.ac.kr

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

요 약

본 논문에서는 눈부신 속도로 발전하는 무선 인터넷 시장에서 무선중계 보안 시스템 설계 시 고려되어지는 단말기의 제약사항을 극복하기 위한 여러 가지 방법들 중에서 응용 계층에서 지원되어지는 방법을 논의하고자 한다. 현재 무선 인터넷 프로토콜은 단말기의 제약 사항 즉, 제한된 처리능력, 작은 메모리, 낮은 대역폭, 배터리 시간 등으로 인하여 유선과 같은 정보보호 수준을 제공하지 못한다. 이를 해결하기 위한 방안이 현재까지도 진행 중이고, 표준화 작업 중에 있다. 이러한 무선 인터넷 프로토콜로는 WAP포럼의 WAP(Wireless Application Protocol), Microsoft사의 ME(Mobile Explore) 또 일본 도코모사의 i-mode가 있다. 현재 전세계적으로 가장 널리 알려진 WAP을 살펴보며, 버전 2.0에서 제시된 응용 계층 전자 서명, 암복호화 함수에 대하여 논의한다. 또한 무선 인터넷 보안에서 빼놓을 수 없는 보안 프로토콜과 그 기반이 될 수 있는 무선 PKI를 간단히 살펴보고, 이와 관련하여 응용 계층에서 전자서명, 암복호화가 무선 PKI와 전송계층 보안 프로토콜에 주는 의미를 논의하고자 한다.

ABSTRACT

In this paper, we discuss about wireless Internet security. The past few years have seen unprecedented growth in the number of wireless user, applications, and network access technologies. Wireless Internet is similar to wired internet, but it has some constrained wireless environment. So many internet technologies for wireless are developing now. There are WAP(Wireless Application Protocol) and WPKI. WAP(now version 2.0) is a protocol specification for wireless communication networks. it provides an application framework and network protocols for wireless devices such as mobile telephones, PDAs and internet technologies. In this paper some analysis of security(e.g. digital signature or encryption) for wireless internet are performed.

키워드
Wireless, 무선 인터넷, WAP, Application

I 서 론

현재 무선 인터넷 서비스는 국내뿐만 아니라 국외적으로 엄청난 속도로 증가하고 있으며, 무선 인터넷 서비스를 사용하는 단말기의 종류로써 이동통신단말기의 경우에는 세계적으로 그 수가 약 60%에 이를 것으로 전망하고 있다. 이에 따라 무선 인터넷에서도 유선과 같은 정보보호 기술이 등장하게 되었는데 아직까지 이동통신 단말기는 개인 PC나 워크스테이션의 성능보다 못하기 때문에, 유선의 정보보호 수준을 무선 인터넷에서는 기대하기는 힘들다. 이를 위해서 많은 정보보호기술 연구가 진행 중이며, 이는 현재 무선 인터넷 프로토콜에 따라 개발 형태가 다르며 두 가지로 나눌 수 있다. 하나는 유선의 형태를 그대로 무선에 적용한 Microsoft사의 ME와 일본의 도코모사 i-mode가 있고, 다른 하나는 무선에 적합한 프로토콜을 새롭게 정의하여 사용하는 WAP(Wireless Application

Protocol)이 있다. 전자의 경우, 유선의 HTTP를 사용하여 전송계층 보안 프로토콜인 SSL(Secure Socket Layer)을 사용하며 유선의 정보보호 메커니즘을 그대로 사용한다. 후자의 경우에는 따로 정보보호 메커니즘을 개발하여 사용하므로 구현이 어렵지만, 무선의 특성을 최대한 고려하여 개발하고 있는 점이 장점이다. 본 논문에서는 WAP에서 제안하는 메커니즘에 대해 논의한다. 먼저 2장에서는 무선 인터넷 프로토콜로써 WAP을 알아본다. 3장에서는 무선 인터넷 보안 프로토콜인 WTLS를 알아보고, 무선 PKI의 고려 사항을 간단히 정리하여 본다. 마지막으로 4장에서는 WAP에서 제공하는 무선 인터넷 보안 기능을 알아보고 결론을 내린다.

II. 무선 인터넷

2.1 무선 인터넷 프로토콜

무선 인터넷이라 함은 이동전화나 휴대용 단말기로 Anytime, Anywhere 인터넷에 접속하여 서비스를 제공하는 것을 말한다. 무선인터넷 기술의 핵심은 휴대용 단말기의 한정된 자원을 감안하고 무선망과 유선망의 효율적인 결합이라 말할 수 있다. 다시 말해서 CDMA/GSM 기반의 무선망과 TCP/IP를 사용하는 인터넷 망을 효율적으로 연동하여, 무선단말기로 무선망을 통해 유선망에 위치한 컨텐츠에 효율적으로 접근할 수 있는 통신 프로토콜을 정의하는 것이 무선인터넷 기술이다.

이러한 무선 인터넷 프로토콜 표준은 국내에서 여러 이동통신 사업자들마다 다른 무선인터넷 프로토콜을 사용하고 있는데, Microsoft의 ME와 WAP 포럼의 WAP을 대표적으로 사용하고 있다.

무선 인터넷 프로토콜 중에서 1997년 6월 Ericsson, Nokia, Motolora 및 Phone.com 등 4개사를 중심으로 WAP(Wireless Application Protocol) Forum을 결성하여 무선인터넷 표준을 제정하고 있는 WAP이 전세계적으로 가장 주목 받고 있으며, 계속해서 표준 제정을 위한 활동을 벌이고 있다. 현재 무선인터넷 서비스 호환을 위한 업계의 대표적인 표준으로 자리잡고 있다.

2.2 WAP의 구조

먼저 WAP은 크게 세 개의 구성 요소 즉, 클라이언트, 서버, 그리고 이 둘 사이에서 중계 역할을 하는 게이트웨이가 있다(그림1). WAP의 핵심요소인 게이트웨이의 역할은 유선의 HTTP를 무선의 프로토콜로 또는 그 반대로 변환 하는 것이다. 무선 인터넷 프로토콜 WAP은 (그림2)과 같이 5개의 계층으로 되어있다. 먼저 WDP는 유선의 UDP와 유사한 비신뢰적인 데이터그램 서비스 계층이고, WTLS는 무결성, 기밀성, 인증 및 부인 봉쇄 서비스를 제공하는 보안 계층이며, WTP는

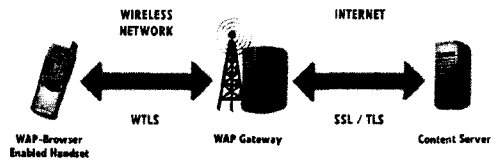

그림 1 WAP 구조[1]

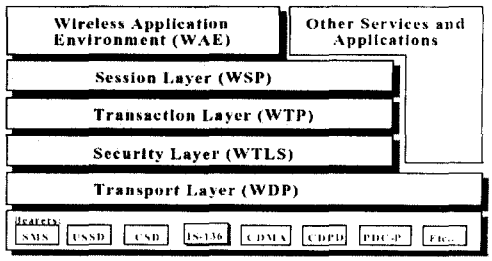

그림 2 WAP 프로토콜 구조

브라우징을 위한 요구 및 응답 형식을 지원하는 Transaction 서비스를 제공하는 계층이다. WSP는 HTTP/1.1에 상응하는 기능의 계층이며, WAE는 무선 인터넷 서비스와 이동전화 서비스를 지원하는 계층이다.

III. 무선 인터넷 보안 프로토콜(WTLS)

무선 인터넷에서 전자상거래를 비롯한 각종 개인 정보나 신용거래 등의 서비스가 안전하게 이루어지기 위해서는 정보보호 문제가 반드시 밑바탕되어야 한다. 정보보호 기술은 기존의 인터넷에서도 가장 중요한 요소로 많은 연구가 이루어지고 있으며, 특히 전자상거래와 같이 개인정보나 경제적인 정보와 관련된 서비스에서 보안은 더욱 중요하다. WAP에서 무선 인터넷 보안 서비스 프로토콜은 WTLS이다. 이는 공개키 교환을 전제로 하고 있는데, 공개키 기반 구조(WPKI)를 사용하여 해결하고 있다. 공개키 기반 구조는 4장에서 다시 업급하겠다. 이번 장에서는 WTLS에서 사용하는 메시지 교환 형식을 살펴보고 제공되는 서비스를 WAP 2.0 스펙으로 살펴보겠다.

먼저 WTLS의 구조를 살펴보면 (그림3)과 같이 레코드, 핸드쉐이크, 경고, 사이퍼스펙 프로토콜 구조를 갖는다. WTLS의 동작 과정은 먼저 양방향에서 키를 생성하기 위하여 헬로 메시지를 교환함으로써 키 재료를 주고 받는다. 여기에는 인증 기관에서 발행한 인증서가 필요하게 되는데 이것은 큰 컴퓨팅 과정이 필요하다. 앞에서도 단말기의 제약

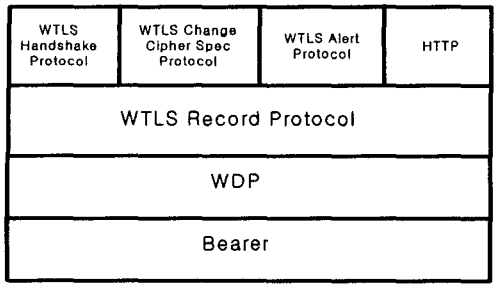

그림 3 WTLS 프로토콜 구조

사항 때문에 인증서 검증과 같은 일은 클라이언트에서 실행하기가 힘들다고 하였다. 이것을 무선에 맞도록 URL을 통하여 검증하는 방법을 권하고 있다. 인증서 정보에서 상대방의 공개키 정보를 가

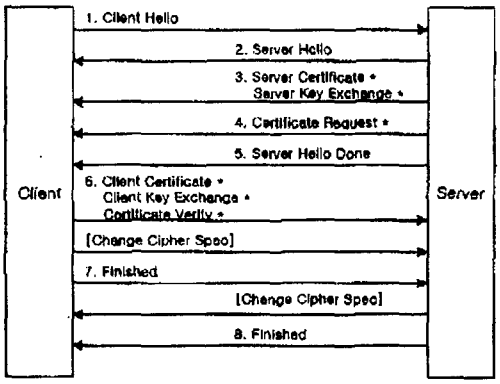

그림 4 WTLS 동작 구조

질수 있고 키 재료 값을 포함하는 암호화 통신 정보를 헬로메시지를 통하여 주고받는다(핸드쉐이크 프로토콜). 그런 후에 키 재료에서 실제 통신에 사용할 키를 만들어 통신을 하게된다(그림4). 또 레코드 프로토콜은 실제 데이터 암호화를 통하여 기밀성과 MAC값을 사용하여 무결성을 제공하고 있다.

WAP 2.0에서는 End-to-End 보안 스펙이 제시되었는데, 무선에 맞는 TCP와 HTTP를 제공하는 WAP HTTP Proxy를 새롭게 추가하고 있다(그림5). 또한 TLS 터널링 구조의 종단간 보안 형태도 제시하였는데, 구조는 (그림6)과 같다. 이는 유선과 같은 종단간 보안 제공을 제시하고 있으며 현재는 미구현 상태이고, 자세한 사항은 참고문헌을 참조하기 바란다. 또 WMLScript Crypto Library를 통하여 응용 계층에서 전자서명 기능을 제공하고 있다. WAP 2.0에서 제공하는 signText함수는 부인봉쇄 서비스를 제공하고 있고, 또 앞으로 살펴볼 암호화 함수도 제공하고 있다. WAP에서 제공하는 보안 요소는 (그림7)에서 볼 수 있다. 또한 WIM(WAP Identity Module)을 통하여

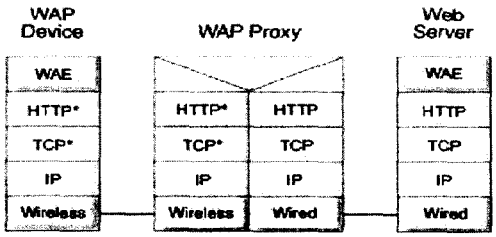

그림 5 Profiled TCP, HTTP를 사용하는 구조[2]

단말기의 작은 저장 공간을 보완하고 있는데, 스마트카드로 구현된 WIM에 비밀키와 인증서를

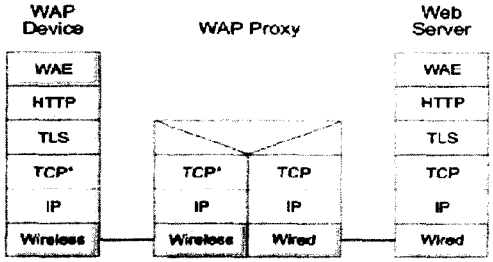

그림 6 TLS 터널링을 사용하는 구조[2]

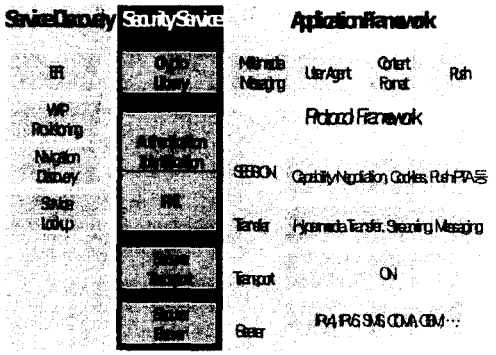

그림 7 WAP 보안요소

저장할 수 있다. 보안 구현 시 중요 고려사항을 살펴보면 PKI에서 가장 기본이 되는 인증서 검증이 제일 비중이 크다. 이는 큰 컴퓨팅 능력을 필요로 하기 때문에 현재의 무선 단말기에는 부담이 되고 이를 해결하기 위하여 인증서의 유효기간을 짧게 사용하는 Shot Lived Certificate (SLC)와 제 3자를 통한 인증서 확인 방법인 Online Certificate Status Protocol(OCSP)을 제안하였다. 참고로 WAP 2.0 모델에서는 유선의 TLS를 지원할 수 있는 외부 장치에서 무선 단말기의 인증서 검증 부하를 분담하여 처리하는 방법이 검토 중에 있고, 사용하는 알고리즘도 기존 RSA보다는 같은 암호학적 강도를 갖으면서 그 크기를 줄일 수 있는 ECC(Elliptic Curve Cryptosystem)를 권장하고 있다.

IV. 무선 PKI

4.1 무선 PKI 고려 사항

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

- 단말기의 메모리 제약을 고려하여 인증기관 간에 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

물론 단말기의 사양도 급속한 발전을 하고 있으므로, 유선 PKI에서 요구하는 처리능력이나 메모리는 곧 극복되리라 예상된다. 이 외에 문제가 발생할 수 있는 단말기 간에 호환성이나 확장성은 현재 국내 WIPI 표준을 통하여 해결을 모색하고 있다.

V. 결 론

전세계적으로 무선 중계보안 시스템 설계에 있어서 가장 기본적인 고려사항은 단말기의 제약사항이다. 급속한 단말기의 발전으로 인하여 현재의 단말기의 제약사항들은 곧 사라질 것으로 예상되지만, 현재 단말기 제약 사항을 바탕으로 하는 무선 WAP 기반의 트랜잭션 보안을 위해서 무선 PKI는 WIM을 사용하여 인증서 검증 부하를 줄이고, 응용 계층에서 전자서명 기능을 제공하거나, 암호화 함수를 사용하여 보다 안전하고, 종단간 보안을 제공할 수 있도록 하고 있다. 현재 WAP 2.0 Security Spec 문서에서는 전자서명 함수와 암호화 함수를 제안해 놓은 상태이다. 그 밖에 무선 PKI를 경량화 시킬 수 있는 함수나 기능을 개발 중에 있다. 또한 국내의 WIPI 표준으로 단말기의 표준화 장치로 개발 효용성도 높여가고 있는 상황이다. Java나 C로 양분화 되어있던 기존의 플랫폼도 두 개의 언어를 모두 지원하기 때문에 두 언어의 장점을 사용한다면 보다 높은 보안 모듈을 개발할 수 있을 것이다.

참고문헌

[1] certicom, Complete WAP Security
[2] WAP 포럼, WAP Architecture
[3] 무선공개키기반구조 표준, WAP-217-WPKI-20010424-a
[4] 한국무선인터넷표준화 포럼, http://www.kwisforum.org
[5] WAP Forum, "Wireless Application Protocol Wireless Transport Layer Security Specification version18-FEB -2000", Feb. 2000
[6] Wireless Application Protocol Wireless Identity Module Specification, WAPFORUM, Feb, 2000.
[7] Entrust, http://www.verisign.com/wireless/index.html
[8] IETF RFC 2560(1996.3), Internet X.509 Public Key Infrastructure Certificate Management Protocols