모바일 인터넷 상의 보안 기법 연구

Research of Security Methods based on Mobile Internet

이원구, 이재광*
한남대학교*

Lee won-goo, Lee jae-kwang*
Hannam Univ*

요약

본 논문에서는 모바일 인터넷에서 보안에 대해 논의한다. 무선 인터넷 사용자나 프로그램 및 네트워크 기술들이 지난 몇 년간 눈부시게 발전했다. 단말기의 제약사항으로 인하여 모바일 인터넷은 유선의 인터넷과 몇 가지 다른 구조를 가지고 있다. 무선 단말기가 갖는 제약 사항으로는 낮은 CPU 처리 능력, 제한된 메모리, 낮은 대역폭으로 유선과 같은 보안 서비스가 이뤄지지 않고 있다. 이를 해결하기 위한 보안 기법에 대해서 논의한다.

Abstract

In this paper, we discuss about mobile 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.

I. 서 론[1)]

최근 인터넷 서비스는 사람 생활의 질을 향상시키는 매체가 되었다. 금융 거래, 지식 검색, 쇼핑 몰등 그 서비스는 사람의 생활 패턴까지도 바꿔놓고 있다. 그러나 과거 인터넷 서비스는 유선에 기반한 서비스로 그 장소가 제한되어 있었지만 현재 모바일 단말기의 보급화로 인터넷을 모바일 통신기기로 즐기려는 수요가 늘고 있다. 이에 발맞추어 여러 무선 인터넷 프로토콜이 생겨나고 표준화가 진행 중에 있다. 본 논문의 2장에서는 무선 인터넷 프로토콜의 개요와 전 세계적으로 대표적이라 할 수 있는 무선 인터넷 프로토콜 WAP (Wireless Application Protocol)을 언급해보며 3장에서는 보안을 담당하는 채널 WTLS (Wireless Transport Layer Security)를 살펴본다. 4장에서는 보안 통신에서 기본이라 할 수 있는 공개키 기반 구조(WPKI)를 살펴보고, 보안을 담당하는 부분에 대해서 논의하고 5장에서 결론을 맺는다.

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

II. 무선 인터넷 프로토콜

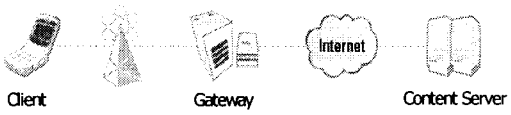
2.1 무선 인터넷 개요

무선 인터넷이란 장소에 상관없이 언제, 어디서나 이동 통신 단말기를 통하여 유선 인터넷과 연결할 수 있는 서비스를 말한다. 무선 인터넷의 구조는 유선의 구조와 비슷하지만, 단말기의 한정된 자원 차이로 무선에 적합하도록 약간의 변경이 있다. 다시 말해서 CDMA/ GSM 기반의 무선망과 TCP/IP를 사용하는 인터넷 망을 효율적으로 연동하여, 무선단말기로 무선망을 통해 유선망에 위치한 컨텐츠에 효율적으

로 접근할 수 있는 통신 프로토콜을 정의하는 것이 무선인터넷 기술이다. 이러한 무선 인터넷 프로토콜 표준은 크게 3가지로 나뉠 수 있는데, Microsoft사의 MME, 일본 DoCoMo사의 i-mode, 그리고 WAPForum의 WAP이 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.

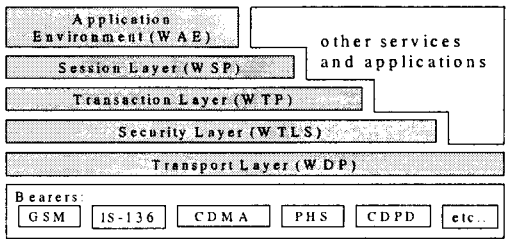
2.2 WAP의 구조

먼저 WAP의 구조는 크게 세 개의 구성 요소 즉, 클라이언트, 서버, 그리고 이 둘 사이에서 중계 역할을 하는 게이트웨이가 있다(그림1). WAP의 핵심요소인 게이트웨이의 역할은 유선의 HTTP를 무선 프로토콜로 또는 그 반대로 변환 하는 것이다.



▶▶ 그림 1. WAP 구조[1]

무선 인터넷 프로토콜 WAP은 (그림2)와 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 브라우징을 위해서 요구 및 응답 형식을 지원하는 Transaction 서비스 계층이다. WSP는 HTTP/1.1에 상응하는 기능의 계층이며, WAE는 무선 인터넷 서비스와 이동전화 서비스를 지원하는 계층이다.

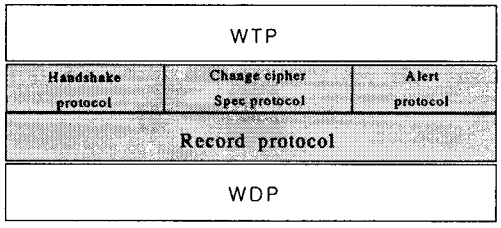


▶▶ 그림 2. WAP 프로토콜 구조

2.3 무선 인터넷 보안 프로토콜(WTLS)

무선 인터넷에서 전자상거래를 비롯한 각종 개인정보나 신용거래 등의 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 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 언급하겠다. 이번 장에서는 WTLS에서 사용하는 메시지 교환 구조를 살펴보겠다.

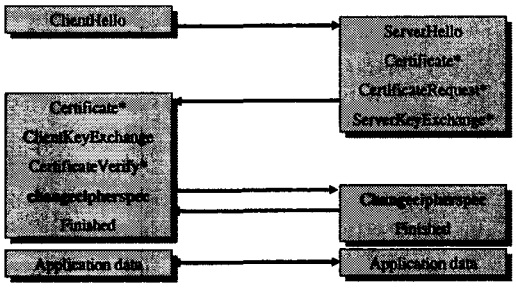
먼저 WTLS의 구조를 살펴보면 (그림3)과 같이 레코드, 핸드쉐이크, 경고, 사이퍼스펙 프로토콜로 구성된다. WTLS의 동작 과정은 먼저 양방향에서 키를 생성하기 위하여 헬로 메시지를 교환함으로써 키 재료를 주고 받는다.



▶▶ 그림 3. WTLS 프로토콜 구조

여기에는 인증 기관에서 발행한 인증서가 필요하게

되는데 이것은 큰 컴퓨팅 과정이 필요하다. 앞에서도 단말기의 제약사항 때문에 인증서 검증과 같은 일은 클라이언트에서 실행하기가 힘들다고 하였다. 이것을 무선에 맞도록 URL을 통하여 검증하는 방법을 권하고 있다. 인증서 정보에서 상대방의 공개키 정보를 가질 수 있고 키 재료 값을 포함하는 암호화 통신 정보를 헬로메시지를 통하여 주고받는다(핸드쉐이크 프로토콜).



▶▶ 그림 4. WTLS 동작 구조

그리고 나서 키 재료에서 실제 통신에 사용할 키를 만들어 통신을 하게 된다(그림4). 또 레코드 프로토콜은 실제 데이터 암호화를 통하여 기밀성과 MAC값을 사용하여 무결성을 제공하고 있다.

Ⅲ 무선 PKI

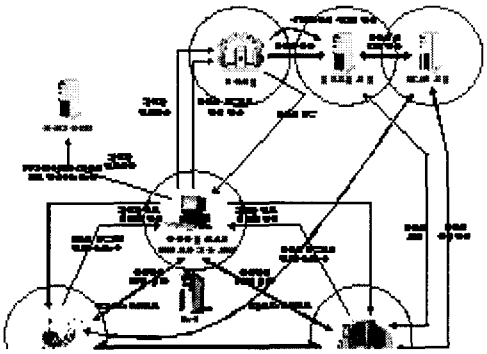
3.1 무선 PKI 고려사항

무선 환경에서 단말기의 제약 사항에 따른 고려사항을 요약하면 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

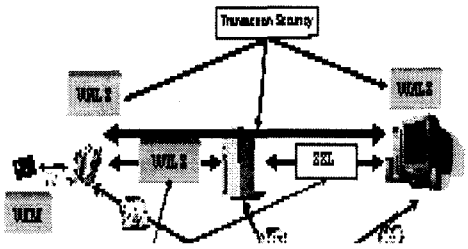
3.2 무선 PKI

휴대폰과 같은 이동 통신 장비가 보급화 되면서 무선 인터넷은 이동성과 편리성을 내세워 엄청난 속도로 발전하고 있다. 그러나 현재 유선과 같은 보안 서비스는 이뤄지지 않고 있다. 따라서 유선과 같은 보안 서비스 즉, 기밀성, 무결성, 인증, 부인방지 등을 제공하면서 무선에 적합할 수 있도록, PKI 구조 변화를 최소화하도록 요구하고 있다. 새롭게 등장한 인증서 검증 방식, 보안 모듈로써 자바 카드 사용, 단대단 보안을 위한 응용계층 전자서명 및 암복호화 함수 사용 등을 예로 들 수 있다. 현재 국내에서는 무선 프로토콜로써 WAP(Wireless Application Protocol)방식과 ME(Mobile Explore)방식을 사용하고 있다. ME 같은 경우는 유선의 HTTP, TCP 프로토콜을 그대로 사용하는 경우이고, WAP의 경우는 무선환경에 적합하도록 만든 프로토콜로 유선과의 연동을 위해서는 WAP Gateway를 두어 유무선간 프로토콜 변경이 이루어져야 한다. 본 고에서는 WAP을 기반으로 하는 무선 PKI를 논할 것이며, 먼저 무선 PKI의 구성요소부터 살펴보도록 한다. 무선 PKI의 구성요소에는 크게 인증서를 발급하고 인증서의 효력정지 및 폐지 기능을 하는 인증기관, 인증 기관과 사용자 사이에서 인증서 등록이나 신원을 확인하는 등록기관, 인증서나 CRL을 저장하는 DB 그리고 사용자로 나눌 수 있다. 현재 WPKI 구조는 (그림1)과 같이 유선의 형태와 비슷하나, 이동통신 단말기의 제약사항으로 인해 자바카드 사용과, 인증서 검증을 위한 OCSP를 사용함으로써 양측간에 인증을 통해서 안전한 통신을 제공한다.



▶▶ 그림 1. WPKI 구조[1]

여기서 보여지는 End-to-End 보안의 개념은 WALS(Wireless Application Layer Security)(그림2) 전자서명 함수 및 암복호화 함수를 사용하여 제공하고 있고, 또 단말기에서 안전한 통신을 위해 보안 모듈(WIM)을 사용하고 있다(그림2). 이는 WAP에서 전송계층 보안을 담당하는 WTLS에서 난수 생성 함수도 지원토록 하고 있으며, 이 난수는 Hello 메시지 교환에 사용되고 양측의 실제 통신하는 암호 알고리즘 키 재료로도 사용된다. 이렇게 단말기에서 WIM을 이용하여 난수 생성 함수와 전자 서명에 사용될 함수가 제공되고 있다. 이는 기존의 단말기의 제약사항을 해결하기 위한 직접적인 방법이라 할 수 있다. 보안모듈을 사용하는 구조는 그림2에서 보듯이 전자 서명을 처리할 수 있고, 암복호화 함수를 제공하여 End-to-End 보안을 제공하고 있다. 다시 말해서 전송 계층의 WIM(Wireless Identity Module)과 응용 계층의 signText 함수와 Encrypt/Decrypt 함수를 사용하여 종단간 보안을 제공하고 있다.



▶▶ 그림 2. 자바 카드를 사용하는 구조

이는 WAP 기반의 보안상 허점인 유무선 프로토콜 변환 시에 평문이 노출되는 위험요소를 해결하여 응용계층 보안 채널을 생성한다.

Ⅳ. 결 론

전세계적으로 무선 인터넷 보안 시스템 설계에 있어서 가장 기본적인 고려사항은 단말기의 제약사항이다. 급속한 단말기의 발전으로 인하여 현재의 단말기의 제약사항들은 곧 사라질 것으로 예상되지만, 현재 단말기 제약 사항을 바탕으로 WAP 기반의 트랜잭션 보안을 위해서는 무선 PKI에 WIM을 사용하여 인증서 검증 부하를 줄이고, 응용 계층에서 전자서명 기능을 제공하고 암호화 함수를 사용하여 보다 안전한 종단간 보안을 제공하도록 해야 한다. 현재 WAP 2.0 Security Spec 문서에서는 전자서명 함수와 암호화 함수를 제안해 놓은 상태이다. 그 밖에 WAPForum의 Working Group에서 무선 PKI를 경량화 시킬 수 있는 함수나 기능을 개발 중에 있으며, 각 이동통신 개발자들로 하여금 직접적인 참여를 권하고 있다. 또한 국내의 단말기의 개발 플랫폼 표준인 WIPI는 각 이동통신사마다 따로 개발하는 불합리한 국내 상황을 하나의 플랫폼에서 개발할 수 있도록 하고 있으며 이는 무선 인터넷 보안 시스템 개발에 원동력으로 제공될 것으로 보인다.

▌참고문헌▌

[1] certicom, Complete WAP Security
[2] WAP 포럼, WAP Architecture
[3] 무선공개키기반구조 표준, WAP-217-W PKI-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
[9] ISTF_022 무선응용계층보안프로토콜 표준
[10] WAP-161-WMLScriptCrypto-200010620-a