자바 기반의 효율적인 무선 보안통신 시스템 분석

채철주*, 김지현*, 이성현*, 이재광*
*한남대학교 컴퓨터공학과
e-mail:cjchae@netwk.hannam.ac.kr

Analysis of Effect on Wireless Security Communication System based on Java

Cheol-Joo Chae*, Ji-Hyen Kim*, Seoung-Hyeon Lee*,
Jae-Kwang Lee*
*Dept of Computer Engineering, Han-Nam University

요 약

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. 단말기의 제약사항으로 인해 무선중계 보안 시스템 설계 시 그 기반이 될 수 있는 무선 인터넷 프로토콜(WAP, I-mode, ME) 중에서 전세계적으로 가장 표준으로 알려진 WAP에 대해서 살펴보고 무선 통신에서 보안 서비스를 위해 사용되는 WTLS와 이를 위한 공개키 기반 구조(WPKI)에서 요구사항을 살펴본다. 실질적으로 무선 인터넷 서비스를 제공하는 자바 보안 기법에 대해서 논의한다.

1. 서론[1)]

현재 무선 인터넷 서비스는 국내뿐만 아니라 국외적으로 엄청난 속도로 증가하고 있으며, 무선 인터넷 서비스를 사용하는 단말기의 종류로써 이동통신 단말기의 경우에는 세계적으로 그 수가 약 60%에 이를 것으로 전망하고 있다. 이동 통신 단말기 보급으로 인터넷 서비스를 받으려는 수요가 생기고, 이에 발맞추어 멀티미디어 서비스를 주축으로 하는 다양한 서비스, 예를 들어 금융거래, 무선 전자상거래 및 위치기반 서비스 등 무선 인터넷 서비스 시장이 급속한 발전을 이루고 있다. 이동 통신 환경에서 이러한 다양한 서비스의 출현은 서비스 공급자나 사용자에게 많은 부가가치를 가져다주고 있으며 이와 함께 정보보호 서비스에 대한 대책도 절실히 요구되고 있다. 또한 유선 상의 정보보호 서비스와는 다르게 무선만이 가지고 있는 환경 즉, 모바일 디바이스의 계산능력의 한계, 주파수 대역 제한, 적은 저장 공간, 배터리 시간 등이 중요하게 고려되어야 할 요소이다. 그러므로 유선인터넷 시스템과 달리 무선인터넷 환경은 여러 가지 제약성을 이유로 유선 시스템에서 사용되던 정보보호 기술을 무선에 적용한다는 것은 아직까지도 매우 어려운 실정이다. 따라서 유선 인터넷에서 이용되는 프로토콜 등을 무선 단말기에 그대로 적용하는 것에는 많은 문제점이 존재하며 이러한 문제점을 해결할 무선 인터넷 프로토콜 기술들이 개발되어졌다. 현재 이동통신 단말기에 탑재되어 응용 프로그램을 수행할 수 있는 환경 즉, 플랫폼에 대해 J2ME(Java 2 Micro Edition)를 간략히 살펴보고 정보보호 기술에 영향을 줄 수 있는 부분을 제안하였다. 따라서 본 논문에서 2장에는 전세계적으로 표준이라 할 수 있는 무선 인터넷 프로토콜 WAP과 무선 보안 프로토콜인 WTLS를 간략히 소개하고, 3장에서는 J2ME에 대한 개요와 정보보호 기술을 제공할 수 있는 J2ME 요소를 조사하고 4장에서는 실질적으로 효과적인 무선중계 보안 시스템

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

에 J2ME가 제공할 수 있는 부분을 제안해보고 향후 연구를 제안하며 본 논문의 결론을 맺는다.

2. 관련 연구

2.1 무선 인터넷 프로토콜

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 효율적으로 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 WAP은 크게 세 개의 구성 요소 즉, 클라이언트, 서버, 그리고 이 둘 사이에서 중계 역할을 하는 게이트웨이가 있다(그림1). WAP의 핵심요소인

그림 1 WAP 구성요소

게이트웨이의 역할은 유선의 HTTP를 무선의 프로토콜로 또는 그 반대로 변환하는 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 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.

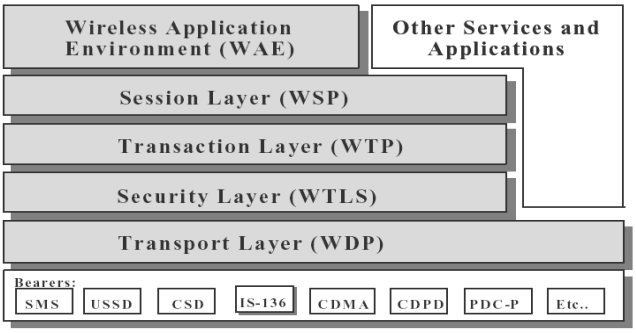

그림 2 WAP 구조

2.3 무선 인터넷 보안 프로토콜

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 업급하겠다. 이번 장에서는 WTLS에서 사용하는 메시지 교환 형식을 살펴보고 제공되는 서비스를 WAP 2.0 스펙으로 살펴보겠다.

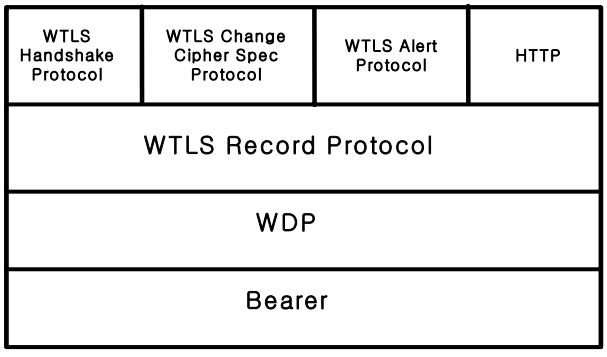

그림 3 WTLS 프로토콜 구조

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 제약사항 때문에 인증서 검증과 같은 일은 클라이언트에서 실행하기가 힘들다고 하였다. 이것을 무선에 맞도록 URL을 통하여 검증하는 방법을 권하고 있다. 인증

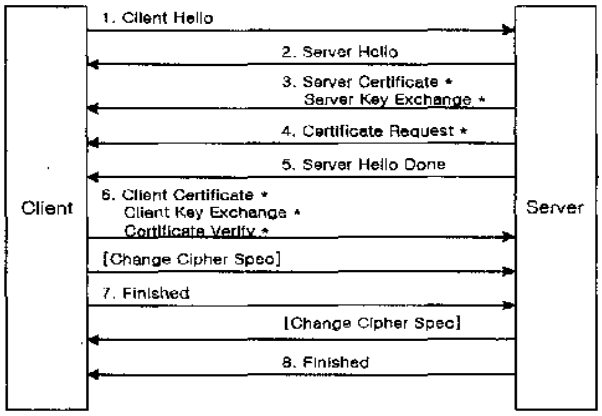

그림 4 WTLS 동작 구조

서 정보에서 상대방의 공개키 정보를 가질수 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. 또한 TLS 터널링 구조의 종단간 보안 형태도 제시하였다. 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. 또한 WIM(WAP Identity Module)을 통하여 단말기의 작은 저장 공간을 보완하고 있는데, 스마트카드로 구현된 WIM에 비밀키와 인증서를 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.

2.3 J2ME

썬 마이크로 시스템사의 자바(Java)를 기반으로 하는 J2ME는 모바일 기기 등에 적합하도록 새롭게 개발한 아주 작은 크기의 자바 애플리케이션 환경을 제공하는 플랫폼이다. J2ME의 구조는 HandHeld Device 나 PDA, ScreenPhone, Set-top Box, net TV와 같은 네트워크로 연결되어 있고, VM 자체가 일반 JVM 보다는 가벼운 VM이 올라가고 또한 그 위에 CoreAPI가 올라가게 되는 구조로 되어 있다. 자바 VM 과 Core API 부분을 CDC 와 CLDC 라는 부분으로 나눌수 있는데, 고정되어 있는 기기들을 위한 CDC, 이동의 개념을 갖고있는 CLDC로 구분지을 수 있다. CLDC는 HandHeld Device을 위한 Configuration이다. CLDC 위에 Profile이라는 부분이 올라가 있는 구조로 실제 제공되는 CoreAPI 이외에 추가적으로 사용될 수 있는 API를 정의하기 위한 부분이다.

3 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 프로토 콜을 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 구성 요소에는 크게 인증서를 발급하고 인증서의 효력정지 및 폐지 기능을 하는 인증기관, 인증기관과 사용자 사이에서 인증서 등록이나 신원을 확인하는 등록 기관, 인증서나 CRL을 저장하는 DB 그리고 사용자로 나눌 수 있다. 현재 WPKI 구조는 유선의 형태와 비슷하나, 이동통신 단말기의 제약사항으로 인해 자바카드 사용과, 인증서 검증을 위한 OCSP를 사용함으로써 양측간에 인증을 통해서 안전한 통신을 제공한다. 여기서 보여지는 End-to-End 보안의 개념은 WALS(Wireless Application Layer Security) 전자서명 함수 및 암복호화 함수를 사용하여 제공하고 있다.

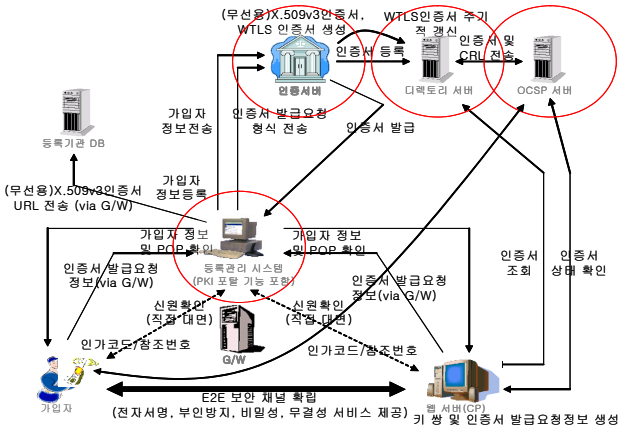

그림5 WPKI 구조

4. 결론

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 J2ME 표준으로 단말기의 표준화 장치로 개발 효용성도 높여가고 있는 상황이다. Java 플랫폼으로 보안상 이점을 최대한 장점을 이용한다면 보다 높은 보안 모듈을 개발할 수 있을 것이다.

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