WIPI 기반의 효율적인 무선중계보안 시스템 분석

최병선, 이성현, 이재광
한남대학교 컴퓨터공학과

Analysis of Effect on Wireless Intermediate Security System based on WIPI

Byung-Sun Choi, Sung-Hyun Lee, Jae-Kwang Lee
Dept of Computer Engineering, Hannam University

요 약

본 논문에서는 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 조사해 보았다. 실질적으로 무선 인터넷 서비스를 제공하기 위한 개발 플랫폼 표준 WIPI(wireless)를 기반으로 무선중계 보안 시스템 중에 WTLS 성능을 향상 시킬 수 있는 부분에 대해서 논의하였다.

1. 서 론

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. 이동통신 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. 추후 본 논문에서 다시 설명하겠으며, 현재 이동통신 단말기에 탑재되어 응용 프로그램을 수행할 수 있는 환경 즉, 플랫폼에 대해 이슈로 떠오르는 있는 WIPI(Wireless Internet Platform for Interoperability)를 상세히 살펴보고 정보보호 기술에 영향을 줄 수 있는 부분을 제안하였다. 따라서 본 논문에서는 2장에서 전세계적으로 표준이라 할 수 있는 무선 인터넷 프로토콜 WAP과 무선 보안 프로토콜인 WTLS를 간략히 소개하고, 3장에서는 WIPI에 대한 개요와 정보보호 기술을 제공할 수 있는 WIPI 요소를 조사하고 4장에서는 실질적으로 효과적인 무선중계 보안 시스템에 WIPI가 제공할 수 있는 부분을 제안해보고 향후 연구를 제안하며 본 논문의 결론을 맺는다.

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

2. 관련 연구

2.1 무선 인터넷 프로토콜

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. 다시

말해서 CDMA/GSM 기반의 무선망과 TCP/IP를 사용하는 인터넷 망을 효율적으로 연동하여, 무선단말기로부터 무선망을 통해 유선망에 위치한 컨텐츠에 효율적으로 접근할 수 있는 통신 프로토콜을 정의하는 것이 무선인터넷 기술이고 해결해야 하는 핵심과제이다.

이러한 무선 인터넷 표준으로는 대표적으로 WAP, I-mode, ME 세가지 프로토콜이 존재하고 있으며, 현재 미국에는 Microsoft사의 ME(Mobile Explorer)가 있고, 일본의 경우에는 i-mode를 사용하고 있고, 우리나라에서는 국내 이동통신 사업자들마다 다른 무선인터넷 프로토콜을 사용하는데, Microsoft의 ME와 WAP 포럼의 WAP을 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 제정한 WAP이 전세계적으로 가장 주목 받고 있으며, 계속해서 표준 제정을 위한 활동을 벌이고 있고, 현재 무선인터넷 서비스 호환을 위한 업계의 대표적인 표준으로 자리잡고 있다.

2.2 WAP의 구조

무선 인터넷 프로토콜인 WAP은 (그림1)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.

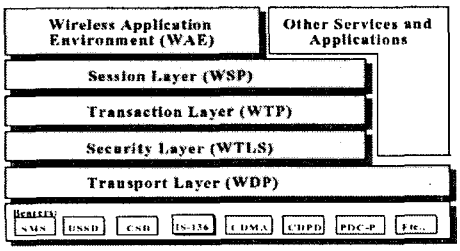

그림 1 WAP 프로토콜 구조

2.3 WAP 정보보안 기반요소(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 서비스에 관련한 프로토콜은 WTLS이다. 물론 이를 위해서 공개키 분배 및 인증에 관한 기반구조가 필요하게 되는데 이를위해 무선 공개키 기반구조(WPKI)를 전제로 하고 있다. 본 논문에서는 WIPI를 기반으로 분석하여 정보보호 기술에 관련된 내용 중에서 무선인터넷 프로토콜인 WAP2.0에서 보안을 담당하는 WTLS에 적용할 수 있는 부분을 논의하고자 하기 때문에 WPKI에서 요구하는 사항은 간략히 내용만 살펴보고, 자세한 사항에 대한 논의는 참고자료에서 확인하도록 한다. 따라서 공개키 교환을 가정 하에 WTLS에서 메시지 교환 형식을 살펴보고 제공되는 서비스는 WAP 2.0 스펙으로 살펴보겠다. 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 있으며 현재 미구현 상태이고, 자세한 사랑은 참고문헌을 참조하기 바란다.

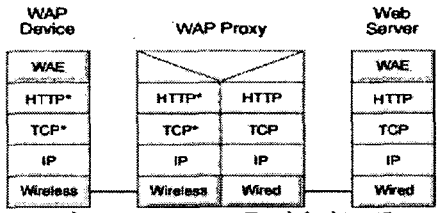

그림 2 TCP, HTTP를 사용하는 구조

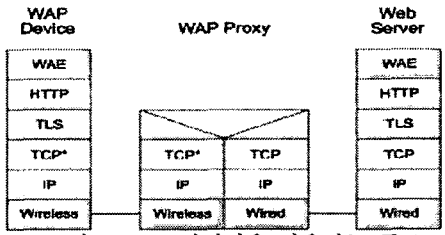

그림 3 TLS 터널링을 사용하는 구조

현재 WAP1.x 버전의 WTLS의 구조가 사용되고 있으므로 그 레코드를 살펴본다. (그림4)와 같이 유선의 SSL의 구조와 유사한 것을 알 수 있다. 데이터그램 프로토콜 WDP 상위 계층에서 작동하고 있으며, helloap서지(그림5)를 통하여 암호화 통신을 위한 세션키 재료를 주고 받게 된다. 레코드 프로토콜은 실제 데이터 암호화를 통해 기밀성과 MAC값을 사용하여 무결성을 제공하고 있다. 또한 WMLScript Crypto Library를 통하여 응용 계층에서의 전자서명 기능을 하는 signText함수[WAP2.0 Spec]를 통하여 부인봉쇄 서비스를 제공하고 있다. 또한 WIM(WAP Identity Module)을 통하여 단말기 제약사항인 적은 저장 공간을 보완하고 있는데, 스마트카드로 구현된 WIM에 비밀키와 인증서를 저장하고 있다. 또한 WTLS에서 이용되는 공개키를 효과적으로 관리하기 위해 IETF의 PKIX WG의 X.509를 기반으로 한 WPKI(Wireless Public Key Infrastructure)를 개발 중이다. 구현에 관련하여 중요 고려사항을 살펴보면 PKI에서 가장 기본이 되는 인증서 검증이다. 이는 큰 컴퓨팅 능력을 필

요로 하기 때문에 현재의 무선 단말기에는 부담이 되고 이를 해결하기 위하여 WAP 1.x 모델에서는 인증서의 유효기간을 짧게 하여 사용하는 Shot Lived Certificate(SLC)와 제 3자를 통한 인증서 확인 방법인 Online Certificate Status Protocol(OCSP)를 도입하였다. 참고로 WAP 2.0 모델에서는 유선의 TLS를

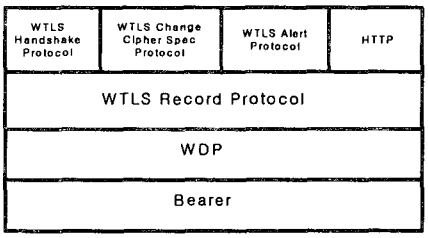

그림 4 WTLS 프로토콜 구조

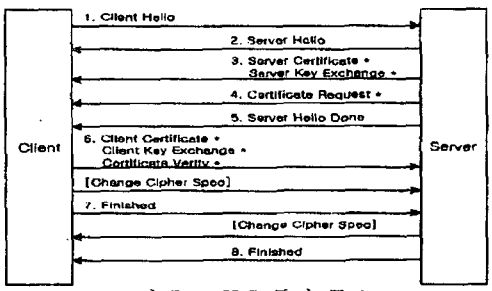

그림 5 WTLS 동작 구조

지원할 수 있는 외부 장치로써 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)을 권장하고 있다.

3. 단말기 개발 플랫폼 개요

휴대폰이나 PDA와 같은 제한된 사양의 모바일 플랫폼에서 동작하는 응용 프로그램을 실행하기 위한 기술로서 가장 대표적인 기술은 퀄컴 사의 BREW (Binary Runtime Environment for Wireless)와 선 마이크로시스템 사의 J2ME(Java 2 Micro Edition)가 있다. BREW와 J2ME는 공통 실행 플랫폼으로서 서로 경쟁하고 있으며, 보통 사용되는 통신 요금과 별도의 요금이 부가되는 부가가치 서비스 및 응용 서비스에 대한 과금 방법을 둘러싼 경쟁도 하고 있다.

개발자 커뮤니티 측면에서는 오래 전에 만들어진 J2ME를 더 선호하고 있는 실정이며. 개발자들은 가상적으로 모든 휴대폰에서 사용될 수 있는 플랫폼을 원하는데, 이런 측면에서 BREW와 자바는 대등한 입장이다. 양쪽 모두 3G 디바이스 위에서 동작하며, 모두 무료 소프트웨어 배포 키트를 제공하고 있다.

3.1 BREW

C언어 개발 플랫폼인 BREW(BREW : Binary Runtime Environment for Wireless)는 퀄컴이 개발한 CDMA 기반 무선기기를 위해 차세대 오픈 플랫폼이다. 기존 플랫폼보다는 무선인터넷용 컨텐츠 개발이 용이하게 하고 있으며, 다양한 플랫폼을 통합한 표준 프로그래밍 환경을 제공해 질적 향상을 도모할 수 있다. 브루 기술이 탑재된 이동통신사의 네트워크를 통해 무선으로 데이터 다운이나 자신의 이동전화기의 소프트웨어까지도 무선으로 업그레이드 할 수 있으며 현재 BREW 2.0으로 명명된 새로운 클라이언트 소프트웨어와 BREW SDK는 무선 전자상거래 활동을 위해 보안 기능을 강화하였고, 무선 인터넷 활동 성능을 확대하고, 더 풍부한 멀티미디어 및 그래픽 기능을 추가하고 있다. 무선 시장에서 BREW 플랫폼을 안전한 플랫폼으로 각인시키기 위한 노력의 일환으로 이전 BREW 플랫폼의 보안 기능을 그대로 기반삼아 만들어 제공하고 있다. 어플리케이션 개발 성능을 증가시킨 것 이외에 BREW 2.0은 무선 모뎀 카드, 저가형 핸드셋 등 메모리가 부족한 다양한 기기에 BREW 플랫폼을 포팅할 수 있는 효율성도 제공하고 있는데, 기기 제조사들은 테이블로 구성된 컴파일링 옵션 (compiling option)을 사용해 쉽게 향상된 BREW 컴포넌트를 제거하고, 표준 BREW 적용을 유지하면서 메모리가 부족한 기기에 필수적인 BREW 콤포넌트만을 선택할 수 있도록 하고 있다.

3.2 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 TV 와 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.

3.3 WIPI

위에서 살펴본 두 가지 C와 JAVA 언어로 양분화되어 무선 응용 프로그램 개발을 하고 있는 국내 상황에 C 언어 개발 플랫폼과 자바 언어 개발 플랫폼을 모두 지원하는 모바일 디바이스 플랫폼 표준인 WIPI(Wireless Internet Platform for Interoperability)는 한국무선인터넷 표준화 포럼(KWISF : Korea Wireless Internet Standardization Forum)의 모바일 플랫폼 특별 분과에서 만든 모바일 플랫 폼 표준 규

격으로서 무선 인터넷을 통해 다운로드 된 응용프로그램을 이동통신 단말기에 탑재시켜 실행 가능하도록 필요한 표준규격을 정의하고 있다.

먼저, 단말기 사양은 급속도로 발전하고 있는 가운데 WIPI에서 요구하는 사양은 <표1>과 같다. 이것은 현재 출시되어지는 단말기 사양은 모두 지원 가능한 단말기들이다. 다음으로 WIPI 플랫폼의 구조(그림6)를 살펴보면, 기본적으로 단말기에 있는 간단한 운영

표 1 WIPI 요구하는 단말기 사양

IO	입력장치 : 키패드 사운드장치 : 진동 및 비프음 네트워크 : 무선 및 시리얼을 통한 전송
ROM	· 플랫폼 library가 사용하는 600KB이상 · 응용 프로그램/관리자가 사용하는 400KB 이상 · 응용 프로그램이 사용하는 시스템 공간 500KB 이상
RAM	· 응용 프로그램이 사용하는 힙 영역 300KB 이상 · 플랫폼 library에서 사용하는 20KB 이상

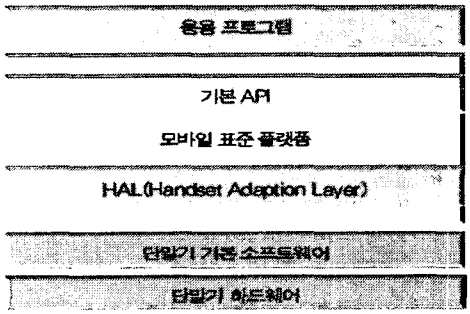

그림 6 WIPI 플랫폼의 구조

체제와 통신 기본 기능 및 각종 디바이스 드라이버를 포함하는 기본 소프트웨어가 있다. 단말기 제조사마다 다른 기본 소프트웨어들이 있겠지만, 단말기 기본 소프트웨어를 추상화 할 수 있도록 하는 HAL 계층을 두어 여러 단말기를 각각의 상이한 단말기로 인식시키는 것이 아니라 표준화된 하나의 단말기로 인식시킬 수 있는 제반 환경을 제공하고 있다. 실질적으로 플랫폼 이식에 하드웨어 독립성을 지원하는 계층이다. 다음으로 기본(Basic) API가 있다. 이것은 C 와 자바 API로 구성되며 기능면에서 동등한 API를 제공한다. WIPI가 규정한 자바 언어용 응용 프로그램도 C 언어 응용 프로그램과 마찬가지로 바이너리로 수행하도록 하고 있기 때문에 속도의 개선 방향을 모색하고 있고, 또 C 및 자바 개발자로 하여금 자유롭게 개발할 여건을 제공하고 있다. 기본적으로 WIPI에서는 플랫폼에 대한 보안도 제공하고 있으며 API보안, 디렉토리 보안을 제공하고 있다. 그 밖에 메모리 관리 및 기타 다국어 지원 등 다양한 규격을 제안하고 제공을 하고 있다.

4. 결론 및 향후 연구

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 위해서는 WIPI에서 제공하는 API 추가/갱신 지원을 통해 효과적인 보안 모듈 등을 동적 라이브러리 형태로 지원하는 방안을 모색할 수 있다. 이것은 WIPI가 가지는 또 다른 강점인 다중언어 지원을 이용하여 각 이동 통신사마다 고유의 API를 자체 개발에 따른 응용 프로그램의 호환성 장애요소 부분을 해결할 것으로 보이며, 더 나아가 공통적으로 필요로 하는 보안 모듈 개발에 대해서도 C와 Java 개발자들로 하여금 최선의 모듈 개발에도 좋은 방법으로 적용할 수 있을 것으로 본다. 향후 연구로는 실질적으로 무선중RP 보안 시스템에서 가장 밑바탕이 될 수 있는 WPKI를 WIPI 환경의 시뮬레이터를 통하여 효과적인 보안 방안을 모색하고 개발해 본다.

[참고 문헌]

[1] 정보통신부, '무선인터넷 표준화 정책방안'

[2] 배석희, '모바일 플랫폼 표준화 동향 및 향후 발전방향', TTA 저널, 제 82호, 2002. 7. 8 20p

[3] 배석희, '모바일 표준 플랫폼 규격(TTAS.KOP-060036)', TTA 저널, 제 82호, 2002. 7. 8, 59p

[4] 한국무선인터넷표준화 포럼, http://www.kwisforum.org

[5] 무선공개키기반구조 표준, WAP-217-WPKI-20010424-a

[6] WAP Forum, "Wireless Application Protocol Wireless Transport Layer Security Specification version18-FEB-2000", Feb. 2000

[7] Wireless Application Protocol Wireless Identity Module Specification, WAPFORUM, Feb, 2000.

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

[9] WAP 포럼, http://www.wapforum.org