WAP에서의 종단간 보안 시스템 설계 및 구현

조영수*, 김명균**

울산대학교 정보통신대학원

Design and Implementation of an End-To-End Security System On WAP

Young-Soo Cho, Myung-Kyun Kim

Graduate School of Information and Communication Technology University of Ulsan

요약

본 논문에서는 WAP 포럼에서 제시하고 있는 무선 인터넷 솔루션인 WAP에서의 보안 메커니즘인 WTLS(Wireless Transport Layer Security), WIM (WAP Identity Module), WMLScript Crypto Library, WPKI(WAP Public Key Infrastructure)에 대해 살펴보고, WAP 게이트웨이를 사용하는 네트워크의 구조적 형태에서 발생되는 종단간 보안 서비스의 문제점에 대해 논의한 후 WAP 환경에서 종단간 보안 서비스를 제공할 수 있는 보안 시스템을 설계 및 구현하고자 한다.

I. 서론

이동통신기술의 발전은 무선 인터넷 사용자의 급속한 증가를 가져왔고, 이러한 증가는 유선 인터넷의 응용서비스 중 증권거래, 계좌이체, 온라인 주문 등의 서비스를 요구하고 있다. 하지만, 이와 같은 서비스를 제공하기 위해서는 무엇보다도 거래의 안전성을 보장할 수 있는 무선 인터넷 보안 기술개발이 선행되어야 한다.[8][9]

현재 무선 인터넷 솔루션에는 WAP 포럼의 WAP, Microsoft사의 ME, 일본 NTT DOCOMO 사의 i-Mode 등이 대표적이며 그 중에서도 WAP이 가장 보편화된 솔루션이다. WAP은 WTLS, WIM, WMLScript Crypto Library 등의 메커니즘을 통해 보안 서비스를 제공하고 있지만 서버와 단말기간에 게이트웨이의 사용은 종단간 보안 서비스를 제공하지 못하는 문제점을 초래했다.[5][6]

본 논문에서는 현재의 WAP 서비스 구조를 유지하면서 종단간 보안 서비스를 제공할 수 있는 보안 시스템을 설계 및 구현하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 WAP에서 제공되는 보안 메커니즘들과 종단간 서비스의 문제점을 분석하고, 3장에서는 종단간 보안 서비스를 제공하기 위한 시스템의 설계 및 구현 방안을 대해 제시하며, 4장에서는 제시한 시스템에 대한 동작 원리 설명과 구현된 시스템에 대해 상술한다. 끝으로 5장에서는 결론을 맺는다.

II. WAP 보안 메커니즘 및 종단간 보안

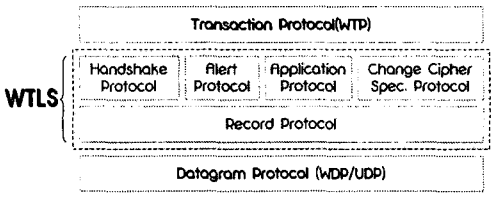
1. WAP 보안 메커니즘

WAP에서는 WTLS (Wireless Transport Layer Security)라고 하는 프로토콜로 데이터의 기밀성, 무결성 및 사용자 인증에 대한 서비스를 제공하고 있으며, 이를 위한 인증서 및 인프라 구축을 위해 WPKI (WAP Public Key Infrastructure)를 제공하고 있다. 또한, 인증서 저장 및 인증서를 위한 키 생성과 저장을 위해 WIM (WAP Identity Module)을 제공하고, 전자상거래의 보안을 위한 중요한 요소인 부인봉쇄 서비스를 위해 응용레벨에서 사용 가능한 WMLScript Crypto Library를 제공하고 있다.

WAP에서 제공하는 보안 메커니즘을 살펴보면,

첫째, WTLS는 HTTP 기반의 인터넷 환경에서 제공되는 보안 서비스인 TLS1.0과 SSL3.0을 기반

으로 무선 환경에 적합하도록 설계되어진 레이어 계층에서의 보안 서비스로 WTP과 WDP 사이에 위치하면서 클라이언트와 서버의 인증 및 세션키 분배를 담당한다. [그림 1]에서처럼 Handshake, Alert, Change Cipher Spec, Application 및 Record 프로토콜로 구성되며 동작 측면에서는 계층적 구조를 가진다. [1] WTLS에서는 데이터의 기밀성, 무결성 및 인증은 보장하지만 부인봉쇄는 제공하지 못하는 문제점을 가진다.



[그림 1] WTLS Protocol

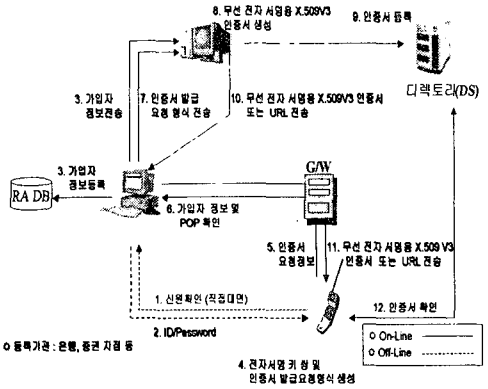
둘째, WIM(Wireless Identity Module)[3]은 무선 단말기의 처리능력을 보완하기 위해 제안된 모델로서 WTLS의 모든 암호 연산을 수행하기 위해 스마트 카드형태로 제공되는 암호 모듈을 나타낸다. WIM을 사용하기 위해서 부가적 스마트 카드 인터페이스가 제공되고 있다. [2]

셋째, WMLScript Crypto Library는 WAP의 WTLS에서 부인봉쇄 서비스를 제공하지 못하는 부분을 응용 레벨에서 전자서명 방식을 통해 부인봉쇄서비스를 제공하는 WMLScript Crypto Library의 Crypto.signText() 함수를 제공한다. 함수의 입력으로는 서명될 데이터, 서명 함수 결과에 추가될 데이터를 의미하는 정수 값, 사용할 서명키를 선택하기 위해 참조하는 값 그리고 그것에 일치하는 서명용 키 아이디를 입력으로 받아서 서명 값 또는 에러 값을 출력한다. [3]

넷째, WPKI는 WTLS와 WIM 같은 규격이 모두 공개키 인증서를 가정하고 있으므로 WAP에서 보안 서비스를 위한 기초를 제공하는 규격이다. [그림 2]는 유선의 공개키 기반 구조를 바탕으로 한 무선 공개키 기반 구조 모델 중 인증서 발급 및 등록 절차를 나타낸 것이다. [4][10]

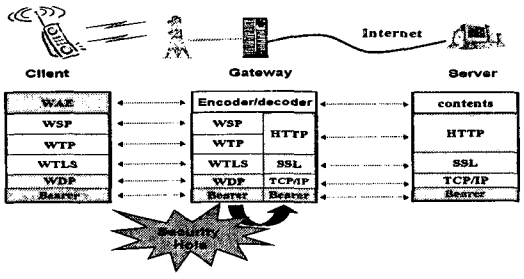
2. WAP에서 종단간 보안[5][6][9][10]

WAP에서 종단간 보안 서비스를 제공하지 못하는 이유는 보안 서비스를 수행하는 WTLS 자체에 문제점이 있는 것이 아니라 무선 구간과 유선 구간을 중개역할을 하는 게이트웨이의 사용으로 인해 발생되는 문제점 때문이다. 게이트웨이는 무선 구간과 유선 구간의 중간에서 프로토콜 변환, HTML 문서를 WML 문서로 변환, WML 문서의 해석(Parsing) 및 이진 부호화(Binary Encoding), 번역(Decoding) 그리고 WMLScript 컴파일 등의



[그림 2] (무선용)X.509V3 인증서 발급신청 및 등록과정 [7]

작업을 수행하는 일종의 서버로서 특히, 유선 구간의 보안 서비스인 SSL과 무선 구간의 보안 서비스인 WTLS 사이의 데이터 변환 작업도 수행하고 있다. 보안상의 문제점은 SSL과 WTLS사이의 데이터 변환 과정에서 사용자의 정보가 게이트웨이 서버에 순간적으로나마 평문으로 노출된다는 것이다. 이에 대한 해결책으로 게이트웨이 서버 자체에 보안을 위한 여러 가지 규정 [7]을 통해 서버 시스템이 구축되고 있지만, 보안상의 문제점을 원천적으로 해결하기 위해서는 종단간 보안 서비스를 제공할 수 있는 시스템이 구축되어야 한다.



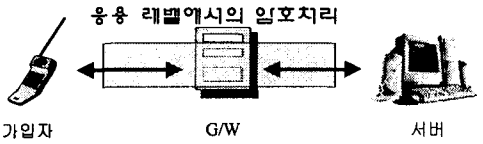
[그림 3] WAP에서 종단간 보안 문제점

WAP에서 종단간 보안 서비스를 위한 방안은

첫째, Secure WAP 게이트웨이를 Web 서버 안쪽의 안전한 도메인 안에 하나를 더 추가하는 방안으로 무선단말기와 Secure WAP Gateway는 WTLS를 통해 서로 통신하도록 구성한다.

둘째, WAP 클라이언트와 WAP 서버간의 응용

레벨에서 데이터를 암호화하여 통신하는 방안으로 [그림 4]와 같다.



[그림 4] WAP에서 종단간 보안서비스 방안 [5]

Ⅲ. 종단간 보안 시스템 설계 및 구현

최근 국내에서는 보안기술 개발업체와 정보보호학회를 중심으로 무선 인터넷 보안을 위한 연구가 활발히 진행되고 있으며, 지난 2001년 8월에는 한국정보보호진흥원에서 무선 PKI 기술규격 안을 발표하여 보안 서비스를 위한 기준을 마련하였다.

종단간 보안 서비스를 제공하기 위해 제안하는 시스템에는

첫째, 공개키 기반의 전자서명 인증서 발급 및 검증 시스템,

둘째, 키 분배용 인증서 발급 및 검증 시스템,

셋째, 종단간 데이터 암호화를 위한 세션키 설립과 데이터를 암호화하여 통신할 수 있는 시스템

등 3가지 시스템이 구현되어야 한다. 하지만 키 분배용 인증서 발급 및 검증 시스템이 전자서명용 인증서 발급 및 검증 시스템과 유사하므로 본 논문의 구현부문에서는 생략하였다.

전체 시스템은 JAVA와 JAVA에서 제공하는 보안 API를 기반으로 하여 클라이언트 / 서버 환경의 시스템을 구축하였으며, 클라이언트 부문은 JAVA 애플릿으로 구현하여 사용자가 사용하기 용이한 화면으로 구성하였다.

1. 전자서명 인증서 발급시스템 [8][10]

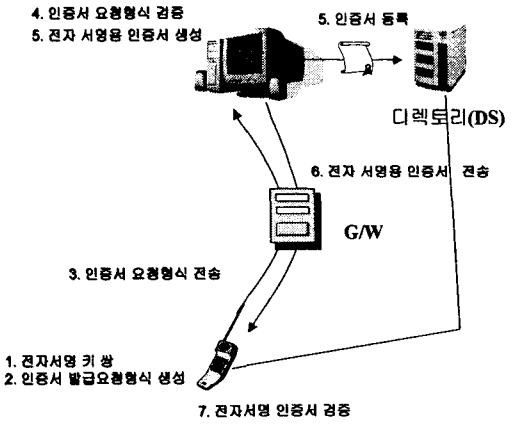
전자서명 인증서 발급 및 검증 시스템에서 쓰이는 아이디와 패스워드는 Off-Line에서 클라이언트와 직접대면 방식을 통해 신원을 확인하고 아이디, 패스워드를 발급하였다고 가정하였다. 또한 인증기관의 공개키 및 비밀키는 사전에 생성되어 공표 되어 있으며, 전자서명 인증서는 X.509 V3을 기반으로 하고, 본 논문에서는 [그림 6]과 같은 구조로 간소화하여 사용하였다.

1.1 전자서명용 키 쌍 및 요청형식 생성

1 단계 : 가입자는 RSA 방식으로 공개키/비밀키 쌍을 생성한다. 생성된 키 쌍은 단말기내에 저장되거나 WIM에 저장되어 사용자의 요청에 따라 사용할 수 있도록 하며, 키 쌍은 PKCS#5으로 암호화하여 PKCS#8 형식으로 저장하는 방안이 제안되고 있다.

2 단계 : 가입자는 전자서명 인증서 요청형식 표준인 PKCS#10, RFC 2511 형식(이름, 아이디, 인증서용도, 공개키 정보, 서명알고리즘)과 POP (Proof of Possession)을 위한 서명 값을 생성한다. 서명 값은 요청형식과 Off-Line에서 발급 받아 보관 중인 패스워드를 함께 축약 방식(SHA-1)으로 축약하여 사용자의 비밀키로 암호화 후 인증기관의 공개키로 암호화한 값이다. 서명 값의 생성은 사용자에 대한 신원확인(사용자 패스워드 사용)과 전송되는 데이터의 기밀성과 무결성을 보장한다.

3 단계 : 사용자는 전자서명 인증서 요청형식과 서명 값을 G/W를 통해 인증기관에 전송한다.



[그림 5] 본 시스템 전자서명 인증서 발급 절차

Version Number
Serial Number
유효기간
공개키 소유자 ID
공개키 정보
서명 값

[그림 6] 본 시스템에서 사용한 인증서 형식

1.2 전자서명용 인증서 생성 및 검증

4 단계 : 인증기관은 수신된 서명 값을 자신의 비밀키로 복호화한 후 사용자의 전자서명 요청형식에 담긴 사용자 공개키로 다시 복호화하여 추출된 축약 값과 수신된 요청형식의 내용, 그리고 인증기관에서 보관하고 있는 사용자 패스워드를 함께 축약하여 나온 값을 비교하여 인증서 요청형식에 대한 검증을 수행한다.

5 단계 : 인증기관은 [그림 7]과 같은 형식으로 사용자 전자서명 인증서를 생성하며, 전자서명 값으로는 전자서명 인증서 내용을 축약한 후 인증기관의 비밀키로 한번 더 암호화한 값을 사용한다. 사용자 전자서명 인증서를 디렉토리 서비스 서버에 공표한다.

6 단계 : 인증기관은 생성된 전자서명 인증서와 서명 값을 G/W를 통해 사용자에게 전송하거나 인증서 URL를 가입자에게 전송한다. 무선 환경에서는 인증서 URL를 사용하는 것이 유리한 방법으로 제안되고 있다.

7 단계 : 사용자는 수신된 인증서 내용을 축약 알고리즘으로 축약하여 생성된 값과 수신된 서명 값의 복호화 (자신의 비밀키로 복호화 및 인증기관의 공개키로 복호화)를 통해 추출된 값을 비교하여 인증서를 검증한다. 인증서 검증이 끝난 인증서는 DER(M)이나 PEM(O) 방식으로 저장하는 것이 표준 규격이다.

2 서버와 클라이언트간 인증서 교환 및 데이터 교환 시스템

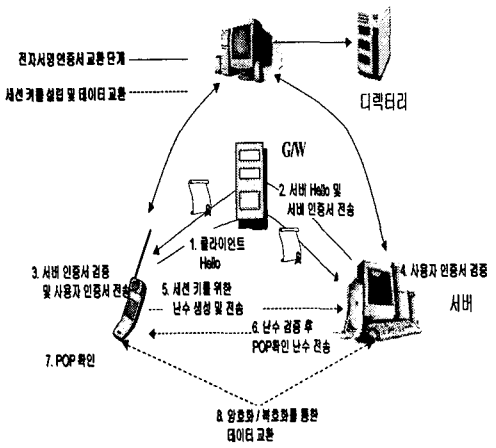
본 논문에서는 전자서명 인증서의 검증을 위해 사용되는 CRL(Certificate Revocation List) 검색이나 OCSP (Online Certificate Status Protocol) 서버를 통한 인증서 상태검증 절차가 제안되고 있지만 본 시스템에서는 인증서의 서명 값, 인증서 유효기간에 대한 확인을 통해 인증서 검증 절차를 대신하였다.

2.1 인증서 교환 및 검증 절차

1 단계 : 클라이언트가 서버에 접속 요청 Hello 메시지를 전송한다.

2 단계 : 서버는 수신된 Hello 메시지에 대해 서버 Hello 메시지와 서버 전자서명용 인증서를 전송하여 데이터 교환을 위한 세션 설립을 사용자에게 통보한다.

3 단계 : 사용자는 수신된 서버 인증서의 서명 값에 대한 확인(서버의 공캐키로 수신된 서명 값



[그림 7] 인증서 교환 /검증 및 데이터 교환

을 복호한 값과 수신된 인증서 내용을 축약 알고리즘으로 축약한 값을 비교)과 유효기간의 확인을 통해 인증서를 검증한 후 사용자 인증서를 서버에 전송한다.

4 단계 : 서버는 수신된 사용자 전자서명용 인증서에 대해 서명 값 확인(사용자의 공개키로 복호한 값과 수신된 인증서의 내용을 축약알고리즘으로 축약한 값을 비교)과 유효기간 확인과정을 거쳐 검증 절차를 마치고, 인증서 교환 완료를 알리는 메시지를 사용자에게 전달한다.

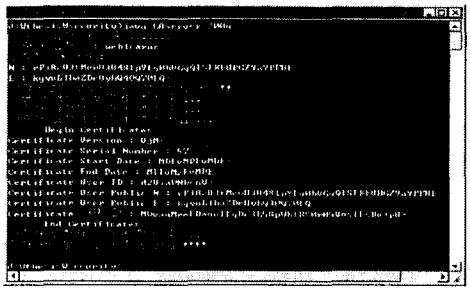
2.2 세션 키 설립 및 데이터 교환 절차

5 단계 : 사용자 단말기에서 세션 키 설립을 위한 난수를 생성하여 서버의 공개키를 이용한 암호화를 통해 서버에 전송한다.

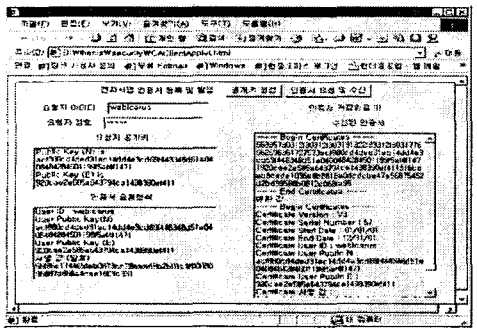
6 단계 : 서버는 수신된 암호문을 자신의 비밀키를 이용하여 복호화한 후 "복호값 + 1"의 값을 생성(POP 확인 값)하고 사용자의 공개키를 이용한 암호화를 통해 사용자에게 전송한다.

7 단계 : 사용자는 수신된 암호문을 자신의 비밀키로 복호화하여 발신한 난수와 비교하는 절차를 통해 유효성이 인정되면 데이터를 암호화하는 비밀키로 사용하는 것을 서버에게 알린다.

8 단계 : 사용자는 생성된 비밀키를 사용하여 데이터를 암호화하여 송신하고 서버는 복호화 과정을 반복하면서 상호간의 데이터를 교환한다.

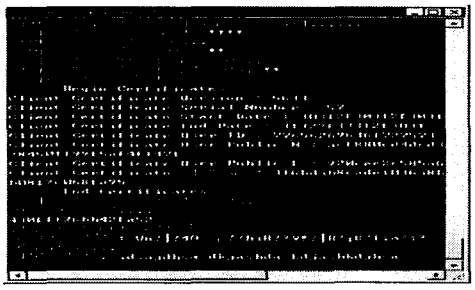


[A] 인증기관

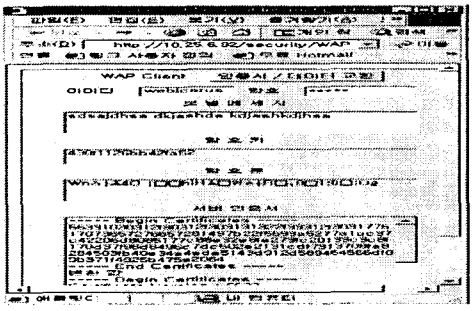


[B] 사용자

[그림 8] 전자서명용 인증서 발급 절차



[A] Web 서버



[B] 가입자

[그림 9] 종단간 보안 서비스 구현화면

V. 결론

본 논문에서는 무선 단말기와 서버간의 종단간 보안 서비스를 제공하기 위한 시스템의 프로토 타입을 구현하였으며, 본 논문에서 사용한 암호화 알고리즘, 인증서 및 인증서 요청형식을 국내 무선 PKI 기술규약에 적합하도록 개선하여 시스템을 구현한다면 기존의 WAP 서비스 모델을 유지하면서도 종단간 보안 서비스를 제공할 수 있는 서비스 모델을 만들 수 있을 것이라 생각된다.

참고문헌

[1] WAP Forum, "Wireless Transport Layer Security", 06-April-2001, http://www.wapforum.org

[2] WAP Forum, "WAP Identity Mo[3] WAP Forum, "WAP Identity Module", 18-Feb-2000, http://www.wapforum.org

[3] WAP Forum, "WMLScript Crypto Library", 20-Jun-2000, http://www.wapforum.org

[4] WAP Forum, "WAP Public Key Infrastructure", 3-Mar-2000, http://www.wapforum.org

[5] Senthil Sengodan, David Smith, Mitri Abou-Ritz, "On End-to-End Security for Bluetooth / WAP & TCP/IP Networks", ICPWC'2000 IEEE, 2000.

[6] Eun-Kyeong Kwon, Yong-Gu Cho, Ki-Joon Chae, "Integrated Transport Layer Security : End-to-End Security Model between WTLS and TLS", IEEE, 2001

[7] Phone.com, "Understanding Security on the Wireless Internet" January. 2000, http://www.phone.com

[8] 문종철, 원유재, 조현숙, "WAP 보안과 표준화 동향", 통신정보보호학회지 제10권 제 2호, 2000. 6

[9] 양종필, 조현호, 이경현, "WAP에서의 새로운 종단간 인증 프로토콜", 한국정보처리학회 춘계 학술발표 논문집 제8권 제1호, 2001.

[10] 이재일, 박정환, 송주석, "WAP을 위한 국내 공개키기반구조(PKI)모델", 통신정보보호학회지 제10권 제4호, 2000. 12