通信情報保護學會誌
第 10 券 第 2 號, 2000. 6

WAP 보안과 표준화 동향

문 종 철*, 원 유 재*, 조 현 숙*

요 약

WAP forum에서 제안한 WAP은 무선 인터넷을 위해 전세계적으로 가장 많이 사용되는 규격으로 무선 환경의 제약성을 고려하여 설계되었다. WAP은 다양한 응용 서비스의 보안을 위해 WTLS, WMLScript Crypto Library, WIM 그리고 WPKI에 대한 규격을 포함하지만 게이트웨이 모델을 사용함에 따른 구조적인 보안 결함을 가진다. 본 논문에서는 WAP 보안을 위한 구성 요소들에 대해 검토하고 현재 WAP 보안의 문제점에 대해 논의한 후 그것을 해결하기 위한 WAP forum의 보안 표준화 방향에 대해 고찰하고자 한다.

Ⅰ. 서 론

GSM, IS-95로 대표될 수 있는 디지털 이동 통신 시스템은 무선망의 발전에 의존해 기존의 음성 통신이나 단문 메시지 서비스를 탈피하여 유선에서 이루어지고 있는 서비스를 무선에서 수용하고자 해 왔으며 완전한 멀티미디어 서비스 제공을 목표로 하는 IMT-2000으로 진화하는 과정에서 현재의 기술을 기반으로 단문 메시지 서비스와는 다른 부가가치(value- added) 서비스를 창출하기 위해 무선 인터넷이라는 개념을 도입하게 되었다.

무선 인터넷은 유선에서만 제공하던 인터넷 접속을 무선 환경에서도 가능하게 해주는 기술이다. 그러나 무선 인터페이스(air interface)는 낮은 데이터 전송 속도, 제한된 주파수 대역bandwidth), 낮은 연결 신뢰성(connection reliability), 제한된 대기 시간(latency) 및 핸드오프(handoff)와 같은 제약성을 가지며 무선 단말기 또한 화면과 메모리, 배터리 및 연산 능력에서 유선의 단말기와는 다른 특성을 가진다. 이러한 제약 조건들은 인터넷을 위해 유선에서 사용하던 프로토콜과 마크업(mark-up) 언어 및 브라우저 등을 그대로 무선 환경에 적용시키는 것을 어렵게 만들었으며 무선 환경에 적합한 새로운 방식의 요구에 따라 게이트웨이(gateway)를 통한 무선 인터넷 모델이 나타나게

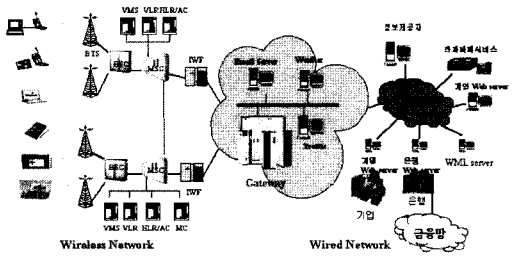


그림 1. 무선 인터넷 개념도

되었다. 그림. 1은 무선망을 이용한 무선 인터넷 개념도를 보여 준다.

이동 통신망은 OSI 계층 중 물리 계층, 데이터 링크 계층 그리고 네트워 계층을 구성하고 있으므로 무선 인터넷 서비스를 위해 베어러(bearer) 위에 세션 및 트랜잭션 컨트롤 기능을 가진 상위 계층이 존재해야 한다. 이러한 상위 계층 프로토콜 중 대표적인 것으로는 WTCP(Wireless TCP)와 WAP (Wireless Application Protocol)이 있는데 IETF (Internet Engineering Task Force)에서 주도하는 WTCP는 기존의 TCP를 이용하여 유선에서 사용되던 응용들에게 호환성을 제공하기 위한 시도로 무선 환경의 제약성을 극복하려는 연구가 아직 진행 중에 있다. 반면 WAP은 무선 단말기에 적합하도록 설계된 무선용 브라우저(browser) 및

* 한국전자통신연구원 정보보호기술연구본부
(문종철 - jcmoon@etri.re.kr 원유재 - yjwon@etri.re.kr 조현숙 - hscho@etri.re.kr)

마크업 언어, 경량화된 세션·트랜스포트 계층, 유무선 연결을 위한 게이트웨이(gateway) 등의 무선 인터넷을 위해 필요한 전반적인 기술을 다루는 사실상의 표준이라 할 수 있다.

전세계적으로 인터넷이 활성화되고 그것을 통한 다양한 응용 서비스가 생겨남에 따라 보안 문제가 심각하게 거론되어 왔다. 특히 인터넷을 통한 뱅킹, 증권 거래 그리고 전자상거래와 같은 서비스에서는 정보의 보호 여부가 서비스 성공과 직결되는 문제라 할 수 있다. 이러한 인터넷상의 보안 문제를 해결하기 위해 많은 방법들이 제안되어 사용되는데 그 중 TCP/IP 위에서 서버와 클라이언트간의 인증 및 세션키 분배를 지원하고 기밀성을 제공하는 SSL (Secure Socket Layer) 및 TLS(Trans-port Layer Security)와 안전한 전자 메일 전송을 위한 PGP(Pretty Good Privacy)를 예로 들 수 있다[1][2][3]. 이와 같이 무선과 인터넷의 결합인 무선 인터넷에서도 정보의 보안 문제는 다른 무엇보다도 중요한데 WAP 규격에서는 WTLS (Wireless Transport Layer Security)라고 하는 프로토콜 계층으로 인증 및 기밀성 문제를 해결하고 있으며 이에 필요한 인증서 및 인프라 구축을 위하여 WPKI (WAP Public Key Infra- structure)를 제안하고 있다[4][5]. 또한 개인 비밀 정보의 안전한 저장을 위해 SIM (Subscriber Identity Module) 카드와 멀티 응용으로 사용할 수 있는 WIM(WAP Identity Module) 스마트 카드 규격 및 부인 봉쇄 서비스를 지원하기 위한 WMLScript Crypto Library 규격을 공개하고 있다[6][7].

본 고에서는 무선 인터넷을 위한 산업체 규격인 WAP에서의 보안 요소에 대해 알아보고 문제점을 고찰한 후 그것을 해결하기 위한 WAP forum의 WAP 보안 표준화에 대해 살펴보고자 한다.

II. WAP 개요

무선 인터넷 서비스를 제공하기 위해 WAP에서 채택한 구조는 게이트웨이 모델이다. 그림. 2에서 보듯이 기본적인 WAP 모델은 무선 사업자가 관장하는 게이트웨이를 중심으로 무선 구간은 WAP을 이용하고 유선 구간은 기존의 인터넷 프로토콜을 사용하도록 구성되어 있다.

WAP 게이트웨이는 무선 구간과 유선 구간의 중간에서 프로토콜 변환, HTML 문서를 WML로 변환, WML 문서의 해석(parsing) 및 이진 부호화(binary encoding), 번역(decoding) 그리고 WMLScript 컴파일 등의 작업을 수행한다. 무선 단말기는 WAP 전용 브라우저를 탑재하고 게이트웨이로부터 이진 부호화되어 수신된 WML 문서를 번역한 후 재구성하여 덱(deck) 단위로 화면에 보여 줄 뿐 아니라 WMLScript를 실행한다. WAP 브라우저에 의해 접근 될 수 있는 형태의 서버는 WML 컨텐츠가 웹 서버를 기반으로 구성되어 있는 경우와 HTML 컨텐츠가 웹 서버에 구축되어 있는 경우이다. 물론 WAP 전용 서버의 가능성도 배제되지는 않는다.

WAP 컨텐트 전송을 위해 필요한 전송 프로토콜은 약간의 차이는 있지만 그림. 3과 같이 인터넷 프로토콜과 비교될 수 있다. 각 프로토콜 스택의 기능을 간단히 살펴보면 다음과 같다.

WDP(Wireless Datagram Protocol)는 트랜스포트 계층의 프로토콜로 상위 계층에 대해 공통의 (common) 인터페이스를 제공하고 하위 계층에 존재하는 트랜스포트 계층을 베어러 서비스의 특성에 적절히 접목시키는 역할을 하며 포트 번호를 관리한다[8]. 또한 필요하다면 세그먼트(segment)와 리어셈블(re-assem ble) 기능 및 에러 검출(error detection) 기능을 제공할 수도 있다.

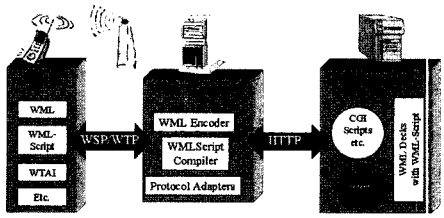


그림 2. WAP 서비스 모델

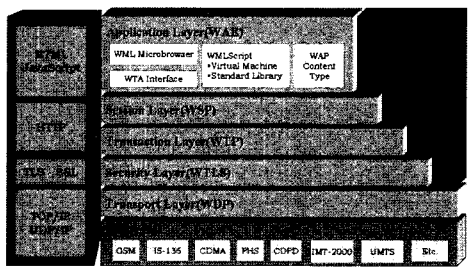


그림 3. WAP 구조

WTP(Wireless Transaction Protocol)는 WDP의 상위 계층 또는 WTLS(Wireless Transport Layer Security)의 상위 계층으로 존재하며 필요에 따라 클래스 0의 신뢰성 없는 데이터 그램 서비스, 클래스 1의 신뢰성 있는 데이터 그램 서비스 그리고 클래스 2의 invoke-response 트랜잭션 서비스를 제공한다[9]. 그리고 클래스 1과 클래스 2의 경우 신뢰성 있는 데이터 전송을 위해 ACK (acknowledge) PDU(Protocol Data Unit)가 수신되지 않으면 정해진 횟수까지 invoke PDU를 재전송 한다.

WSP(Wireless Session Protocol)는 개념적으로 WTP 위에서 동작하여 연결 지향(connection-oriented) 서비스를 제공할 수도 있고 WDP 위에서 동작하여 연결 없는(connectionless) 서비스 제공이 가능하다[10]. WSP는 클라이언트와 서버간의 세션 설정을 위해 동작하는 프로토콜인데 기본적으로 HTTP1.1(HiperText Transfer Protocol)에 기반한 시멘틱(semantic)과 메커니즘(mechanism)을 제공하며 세션을 임시 중단(suspend)하고 다시 시작(resume)하는 기능을 제공한다.

WAE(Wireless Application Environ- ment)는 WML(Wireless Mark-up Language), WMLScript, 마이크로브라우저(microbrowser)로 구성되어 있으며 중요한 기능으로는 이진 부호화된 WML의 번역, WMLScript의 실행, 컨텐트 포맷팅(content formatting) 등이 있다[11].

WTLS는 WAP의 전체 보안을 담당하는 계층으로 다음 장에서 그 의미와 문제점을 살펴보고 WAP 보안과 관련된 다른 부분들을 고찰하도록 한다.

Ⅲ. WAP 보안

WAP에서 보안과 관련된 요소는 WTLS와 WMLScript Crypto Library, WIM 그리고 WPKI 이다.

WTLS는 WAP 프로토콜 스택의 WTP와 WDP 사이에 위치하면서 클라이언트와 서버의 인증 및 세션키 분배를 담당하고 WPKI는 무선 환경에 적합한 공개키 기반 구조를 제공한다. 그리고 WIM은 사용자 데이터의 안전한 저장을 위해 존재하는 요소로 스마트 카드로 구현되어 WTLS와 WMLScript Crypto Library에서 필요한 암호 연산을 지원하고 비밀키 및 인증서를 저장한다. WMLScript Crypto Library는 WTLS에서 지원할 수 없는 전자 서명 메커니즘으로서 응용 레벨(level)에서 트랜잭션의 인증 및 부인 봉쇄 서비스를 제공한다.

1. Wireless Transport Layer Security 프로토콜

WTLS는 유선에서 사용하는 SSL/TLS와 비슷한 구조를 가지면서 무선 환경에 적합하도록 설계된 프로토콜이다. 그림. 4에서 보는 것처럼 WTLS는 handshake, alert, Change Cipher Spec 그리고 Record 프로토콜로 구성되고 동작 측면에서 계층 구조를 지닌다.

Handshake 프로토콜은 WTLS 세션이 설정될 때 가장 먼저 이루어지는 프로토콜로 구현 클래스 3으로 구현될 때 암호학적으로 AKC (Authenticated Key establishment with key Confirmation) 프로토콜이라 할 수 있으며 클라이언트와 서버의 인증 및 암호 알고리즘 그리고 암호화 키 설립이 이 과정에서 일어난다[12].

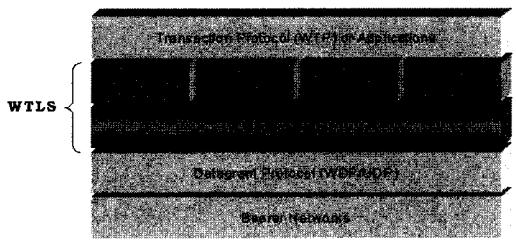


그림 4. WTLS 프로토콜

Handshake 프로토콜에는 full handshake, abbreviate handshake 그리고 optimized handshake의 3 가지가 있는데 일반적으로 세션을 처음 설립할 때 full handshake가 사용되고 같은 세션을 다시 열고자 할 때는 abbreviate handshake 그리고 키 설립 방식이 ECDH (Elliptic Curve Diffie-Hellman)로 결정되었고 ECDSA (Elliptic Curve Digital Signature Algorithm)로 서명된 인증서를 교환할 필요가 있을 때 서버가 자신의 자원(source)으로부터 클라이언트의 인증서를 얻을 수 있다면 optimized handshake가 사용된다. 그림. 5는 full handshake 프로토콜을 보여 준다.

ClientHello 및 ServerHello 메시지는 랜덤수(random number)와 암호 알고리즘을 협상하는 단계이며 여기서 설정된 키 교환 메커니즘에 따라 handshake 프로토콜의 메시지 및 프로토콜 단계가 조금씩 달라지게 된다. Hello 메시지를 교환한 후 서버와 클라이언트는 인증서를 교환하고 키 공유를 위해 필요한 파라미터를 설정한다. 그리고 나서 프리마스터 키(premater key)를 공개키 연산을 통해 공유하며 암호 알고리즘을 사용하여 세션키인 마스터 키와 그것으로부터 유도된 암호 및 MAC (Message Authentication Code)용 키 블럭(block)을 생성한다. 첫 번째 키 블럭은 Change CipherSpec 메시지를 주고 받은 후 바로 계산되며 키 갱신(key refresh) 파라미터와 시퀀스 넘버(sequence number)에 기반해서 연결(connection) 중에 갱신될 수 있다.

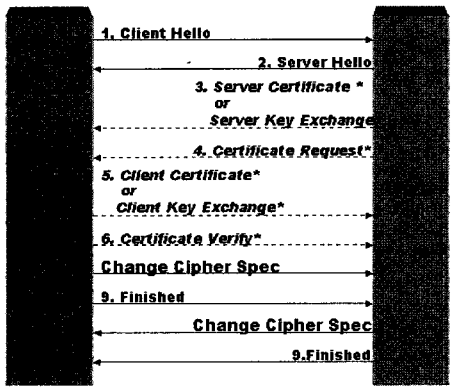


그림 5. Full handshake 프로토콜

Change Cipher Spec 프로토콜은 handshake 과정에서 알고리즘 및 키가 협상되었고 Record 프로토콜에서 사용될 모든 보안 파라미터(security parameter)들이 설정되었을 때 handshake 프로토콜을 끝내기 위한 Finished 메시지를 보내기 전 현 시점부터 보안 파라미터를 사용함을 상대방에게 통보하기 위해 사용된다. Finished 메시지는 키 확인(key confirmation) 및 handshake 프로토콜 메시지의 무결성을 확인시켜 준다. Hand- shake 프로토콜에서 설정된 보안 파라미터들인 세션 아이디(session id), 암호 알고리즘, 키 갱신 파라미터, 랜덤수, 마스터 키 등을 이용하여 생성된 연결 상태 파라미터(con-nection state parameter)를 참조하면서 Record 프로토콜은 메시지를 압축하고 MAC을 연결한 후 그것을 암호화해서 전송한다.

WTLS는 RSA, DH, DES, IDEA, SHA-1 등 다양한 암호 알고리즘을 사용하고 있으며 유한체상의 인수분해 문제나 이산대수 문제에 기반한 공개키 알고리즘과 동등한 안전성을 보장하기 위해 보다 작은 키 길이를 가지면서 빠르게 동작할 수 있는 타원 곡선(elliptic curve) 공개키 암호 알고리즘을 포함하고 있다[13].

WTLS는 휴대 단말과 게이트웨이에 포팅(porting)되어 무선 구간의 트랜스포트 계층에서 데이터 기밀성 및 무결성을 보장해주지만 단대단 보안을 위해 게이트웨이에서 프로토콜 변환을 거쳐 유선의 SSL과 연결되는 동안 암호화된 데이터가 평문으로 복호되는 결함을 가진다. WAP forum에서는 이 문제를 해결하기 위해 트랜스포트 레벨에서 WTLS를 이용한 운영 메커니즘을 새로이 제안하고 있지만 아직 승인된 규격은 아니다.

2. WMLScript Crypto Library

WTLS는 WAP 채널 보안을 위해 인증 및 암호화 기능을 제공하지만 응용 레벨에서 반드시 필요한 것으로 여겨지는 전자 서명을 지원하기 위한 메커니즘은 가지고 있지 않다. 이것은 국내에서 볼 때 WTLS가 전자 서명법의 테두리에 있지 않음을 의미하며 보안 측면에서도 부인 봉쇄 서비스가 제공되지 않으므로 무선 전자 상거래나 무선 뱅킹 등에서 치명적인 문제점을 야기할 수 있다. 이러한 문제점을 인식해 WAP forum에서는 응용 레벨에서 전자 서명을 지원하기 위한 방식으로 스크립트에서 사용하기 위한 전자 서명 함수를 제안하고 있다.

WMLScript Crypto Library 규격에서 전자 서명을 위해 제공되는 Crypto.signText 함수는 입력으로 서명될 데이터, 서명 함수 수행 결과에 추가될 데이터를 의미하는 정수값, 사용할 서명키를 선택하기 위해 참조하는 값 그리고 그것에 일치하는 서명용 키 아이디(ID)를 입력으로 받아서 서명 값 또는 에러 메시지를 출력한다. 이때 서명용 키는 무선 단말기에 저장되어 있을 수 있으며 WIM에 저장되어 있을 수도 있다. 서명을 증명하기 위해 서버는 클라이언트의 인증서를 필요로 하는데 서명값에 직접 추가되어 전달되거나 URL(Uniform Resource

Locator)을 참조하여 인터넷을 통해 가져 올 수도 있다.

3. WAP Identity Module

WIM은 무선 단말기의 하드웨드 및 소프트웨어의 보안 취약성을 보완하기 위해 사용하는 암호 모듈(cryptographic token)이라 볼 수 있다. 무선 단말기는 일반적으로 processor, data/address bus, flash ROM(Read Only Memory), RAM (Random Access Memory), EEPROM (Electrical Erasable Programmable ROM), 무선 모뎀(Mobile Station Modem)과 실시간 OS (real time OS) 및 MSM 구동 소프트웨어 등으로 구성되는데 이러한 모듈들은 일반적으로 물리적(physical) 및 논리적(logical) 공격 방지 기법을 적용하지 않는 한 DPA (Differential Power Attack)과 같은 em- bedded system에 대한 공격에 취약한 것으로 알려져 있다[14].

스마트카드는 비록 이상적인 tamper-proof 장치(device)는 아니지만 알려진 물리적 공격과 논리적 공격에 대해 대비하여 하드웨어 및 소프트웨어가 구현되기 때문에 개인의 비밀 정보를 저장하는 가장 안전한 매체중 하나로 볼 수 있다. GSM에서는 이미 SIM 카드로 불리는 스마트카드를 개인 정보 저장과 사용자의 이동성 보장을 목적으로 사용해오고 있다.

WAP을 위한 스마트카드인 WIM은 접촉형 카드 규격 ISO/IEC7816과 암호 토큰 정보 포맷을 정의한 PKCS15 그리고 SIM을 위한 GSM11.11 등의 규격을 따르면서 WTLS에서의 암호 연산 및 응용 레벨에서의 서명을 지원한다[15][16][17].

WTLS에서 WIM이 사용되는 경우는 클라이언트 인증서를 요구하는 RSA handshake 프로토콜과 abbreviated handshake가 이루어질 때 그리고 optimized ECDH_ECDSA handshake 프로토콜이 이루어 질 때이다. 이 경우 WIM은 WTLS의 record 프로토콜에서 이루어지는 데이터 암호화 및 MAC 연산을 제외한 모든 암호 연산을 수행하게 되는데 이때 WIM 외부로 암호화 키 및 MAC용 키가 전송되는 단점을 가지고 있다.

현재의 스마트카드와 외부 인터페이스의 데이터 교환은 문자(character) 및 블럭(block)에 기반한 비동기 half-duplex 전송 프로토콜을 사용하므로 데이터 교환 속도에 한계가 있다. WIM에서는 T=0 프로토콜을 사용할 경우 대략 9600 bps의 일방향 전송 속도를 기본으로 구현할 것을 제안하고 있다. 이렇게 볼 때 record 프로토콜의 동작을 위해 외부 메모리(memory)에 존재하는 데이터의 암호화 및 MAC 생성을 WIM이 수행하여 값을 되돌려 주는 것에는 카드의 수행 속도가 문제라기 보다는 오히려 데이터 전송 속도 때문에 전체 프로토콜 수행 능력이 저하될 가능성이 존재한다. 그러나 스마트카드 내부에 UART (Universal Asynchronous Reciever Trans- mitter)와 같은 하드웨어 모듈이 구현되고 full-duplex 전송 프로토콜이 실현된다면 WIM에서 WTLS의 모든 암호 연산을 수행하는 것이 바람직할 것이다.

4. WAP Public Key Infrastructure

WTLS와 WMLScript Crypto Library와 같은 규격이 모두 공개키 인증서를 가정하고 있으므로 무선 공개키 기반 구조는 WAP에서 보안 메커니즘을 구현하기 위한 기초가 된다고 할 수 있다. 그러나 현재 무선 공개키 기반 구조와 관련해 WAP forum에서 승인한 규격(approved specification)은 없으며 2000년 3월 WAP forum이 공개한 WAP Certificate and CRL Profiles 규격은 아직 제안 단계에 머물러 있는 상태이다[18].

WAP Certificate and CRL Profiles 규격은 WAP 인증서가 가능한 작은 크기(size)를 가지고 최소의 처리 시간을 유지하면서 보안성 및 호환성에서는 이미 존재하는 기반 구조를 따를 것을 요구한다. 이러한 요구 사항을 고려해 WAP Certificate and CRL Profiles 규격에서는 인증(authentication)을 위한 사용자 인증서, 디지털 서명(digital signature)를 위한 사용자 인증서 그리고 CA 인증서 및 CRL(Certificate Revocation Lists) 프로파일(profile)에 대해 기술하고 있다.

WTLS에서 클라이언트 인증을 위해 사용되는 사용자 인증서는 그림. 6과 같으며 무선 단말은 적어도 700 바이트 크기를 가진 인증서까지를 처리할 수 있어야 한다.

WAP 무선 공개키 기반 구조에서 제안하는 인증서와 WTLS에서 제안하고 있는 WAP 인증서의 데이터 구조와 다른 점은 일련 번호 필드(serial number field)와 확장(extension) 필드의 존재

이다. 일련 번호는 인증서 일련 번호를 의미하며 64 비트를 넘지 않아야 한다. Signature(algorithm) 필드는 인증서에서 사용된 서명 알고리즘을 나타내기 위해 사용되는데 sha1WithRSAEncryption 또는 ecdsa-with-sha1을 위한 object identifier로 채워진다. issuer와 subject 필드는 인증서의 발행자 이름(name)과 인증서 소유자 이름으로 구성된다. validity 필드는 인증서의 유효 사용 기간을 의미하며 subjectPublic KeyInfo 필드는 인증서 소유자의 공개키가 RSA 형태인지 아니면 타원 곡선 암호 시스템의 점(point)인지를 파라미터와 함께 나타낸다. Signature(value) 필드는 인증서에 있는 데이터를 signature(algorithm) 필드의 알고리즘을 이용해서 계산한 서명 값으로 채워진다.

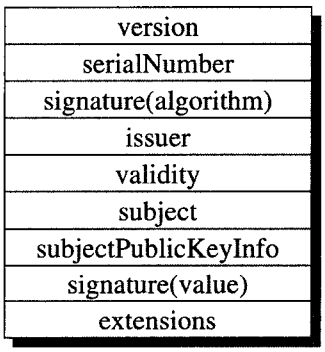


그림 6. 사용자 인증서

Extension 필드의 내부는 그림. 7과 같이 많은 필드로 이루어지는데 그 중 인증서를 처리하는 응용 프로그램이 반드시 인식해야 하는 필드는 Key Usage, Certificate Policy, Subjet Alternative Name, Basic Constraint 그리고 extended Key Usage 필드이다.

디지털 서명을 위한 사용자 인증서는 Crypto. signText()에 의해 계산된 서명값의 증명을 위해 사용되는 인증서로 Key Usage 필드의 비트 중 전자 서명 또는 부인 봉쇄 비트가 표시되는 것을 제외하면 인증을 위한 사용자 인증서와 같은 형태를 가진다. 또한 CA 인증서도 Key Usage 필드의 keyCertSign 비트가 표시되고 Basic Constraint 필드중 cA 구성 요소(component)가 TRUE가 되고 pathLenConstraint 구성 요소가 필요하지 않다는 것을 제외하면 인증을 위한 사용자 인증서와 같다.

WAP forum은 CRL 프로파일에 대한 특별한 규격을 제시하지 않고 있으며 단지 X.509 인증서 CRL을 무선 환경을 통해 전송하지 말 것과 유선에서의 CRL 프로파일을 권장하는 정도에 머물고 있다.

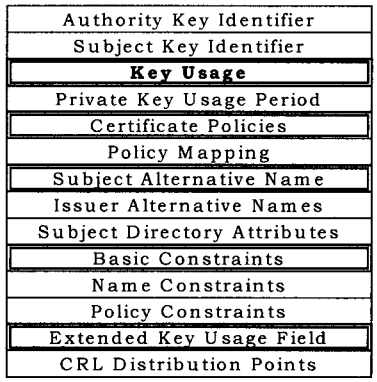


그림 7. 인증서 확장 필드

비록 WAP forum에서 제안한 무선 공개키 기반 구조 관련 규격이 아직은 미비하지만 내부적으로 유선에서의 공개키 기반 구조를 크게 변형하지 않는 방향으로 작업이 이루어진다면 머지 않아 산업체의 요구를 반영한 규격이 제정될 것으로 여겨진다

Ⅳ. WAP 보안 표준화 동향

무선 인터넷 시장을 선점하기 위해 스웨덴의 Ericsson, 핀란드의 Nokia, 미국의 폰닷컴 등은 독자적으로 무선용 프로토콜을 개발하기 시작했으며 각각 ITTP(Intelligent Terminal Transfer Protocol), TTML (Tag- ged Text Mark-up Language) 그리고 HDTP(Handheld Device Transport Protocol)을 완성하였으나 사용에 있어서 호환성에 문제점을 드러내었다. 그리하여 Ericsson, Motorola, Nokia, Phone.com 4개사는 무선 인터넷 및 진보된 무선 데이터 서비스를 위한 국제적 무선 프로토콜 개발과 무선용 컨텐츠 및 응용의 개발을 목표로 1997년 6월 WAP forum을 창립하였다. WAP forum은 현재 전세계 200여개의 단말기 제조업체, 이동 통신 사업자, 컨텐츠 제공자(Contents Pro- vider)들을 회원으로 하고 있으며 WAP 버전 1.2를 공개하고 있다.

WAP에서 보안과 관련한 규격은 1999년 11월 WTLS, WIM, WMLScript Crypto Library 버전 1.2가 승인되었으며 인터넷을 통해 공개되었다. 그러나 2장에서 살펴보았던 것처럼 이 규격들은 나름대로의 문제점을 안고 있으며 명확하지 않은 문구로 표현된 부분들이 존재하고 있어 WAP forum에서는 갱신된 규격을 준비중에 있다. 새로이 제정될 버전 1.3의 보안 관련 규격은 무선 공개키 기반 구조를 추가할 것으로 예상되며 그것과 관련해 WAP forum에서 제안하고(propose) 있는 것은 WTLS와 WIM, WAP Certificate and CRL Profile 그리고 WTLES(WAP Tran- sport Layer End-to-End Security) 규격이다[19].

새로이 제안된(proposed) WTLS 규격에는 버전 1.2의 에러 경고(alert) 메시지 중 현재 보안 세션이 설립되지 않았음을 알리지 위한 no connection 경고에 대해 sequence number와 연관된 부분과 record를 수신하지 않은 상태에서 경고 메시지를 보내는 방법이 추가되었고 Saarinen의 unauthenticated alert message에 대한 서비스 거부 공격(denial of service attack)을 피하기 위해 이 데이터의 sequence number를 유효한 것으로 받아들이기 전에 checksum을 확인하도록 하고 있다[20]. 그리고 클라이언트 인증을 위해 인증서 URL를 사용하는 부분이 추가되었다.

WIM 규격에서는 WIM이 사용되는 부분에 대한 규정에서 공개키 기반 구조의 클라이언트 기능을 위한 WIM 사용을 제한하고 있으며 WIM의 정보 객체(object)에 접근하기 위한 조건을 명확하게 나타내고 있다. 또한 응용 선택(application selection)을 위한 명령 APDU(Application Protocol Data Unit)을 보다 명확히 하고 있으며 간접적으로 응용을 선택하지 않도록 하고 있다.

무선 공개키 기반 구조와 관련해서 WAP forum는 WTLS 클래스 2와 클래스 3 그리고 signText 함수를 사용할 경우에 대해 무선 공개키 기반 구조의 모습을 대략적으로 보여 주고 있다. WAP forum 내부 문서에서는 유선의 RA(Registration Authority)와 비슷한 역할을 하는 PKI portal을 정의하고 있으며 게이트웨이 인증서에 대해 24시간 정도의 짧은 유효기간을 가지도록 하여 클라이언트가 CRL 검증을 피하는 방법을 논의하고 있다. 그리고 신임하는 CA(trusted Certificate Authority) 정보를 다루는 방법이나 클라이언트 등록(registration)과 같은 운영에 관련된 부분도 다루고 있다. 그러나 WAP forum에서도 아직 공개키 기반 구조의 구체적 규격을 제시하지는 못하고 있으므로 완전한 WAP 공개키 기반 구조 규격이 제정되기 전까지는 유선의 공개키 기반 구조를 기반으로 무선 구간에서 서비스가 이루어 질 것으로 예상된다. 그림. 8은 유선의 공개키 기반 구조를 바탕으로 한 무선 공개키 기반 구조 개념도이다.

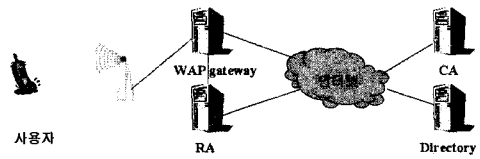


그림 8. 무선 공개키 기반 구조 개념도

WTLES 규격은 2 장에서 언급했던 WAP의 구조적 문제에 의한 WTLS의 문제점을 응용 레벨이 아니라 트랜스포트 계층의 WTLS로 해결하고자 하는 시도로 볼 수 있다. 그림. 9는 WTLES의 논리적 구조를 보여 주고 있다.

WTLS로 단대단 보안을 실현하는 과정을 살펴보면 대략 다음과 같다. 먼저 클라이언트가 trusted master pull proxy를 통해 접속을 원하는 응용

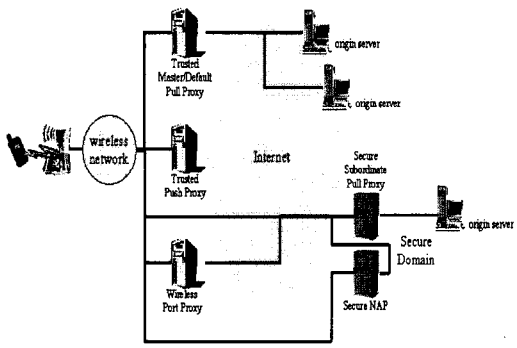


그림 9. WTLES 구성도

서버에 접속했을 때 응용 서버는 클라이언트가 자신의 secure subordinate pull proxy를 통해 접속할 수 있다는 것을 의미하는 에러 코드와 관련 정

보를 trusted master pull proxy에게 보내고 trusted master pull proxy는 관련 정보에 대한 유효성 검토를 거쳐 클라이언트에게 전달한다. 클라이언트는 secure subordinate pull proxy에 접속하여 WTLS 세션을 설립하고 암호 통신을 시작한다. 이러한 단대단 보안 방식은 클라이언트가 사업자 영역에 있는 master pull proxy를 절대적으로 신뢰할 수 있어야 한다는 점에서 문제가 제기될 수도 있다. 만약 pull proxy가 잘못된 접속 정보를 클라이언트에게 전달한다면 클라이언트는 제 3 의 서버와 WTLS 세션을 맺을 가능성이 존재하기 때문이다.

V. 결 론

지금까지 우리는 무선 인터넷에서 산업체 규격이라 할 수 있는 WAP의 보안 방식과 문제점 그리고 이것을 해결하기 위한 WAP forum의 표준화 동향에 대해 살펴보았다. WTLS는 WDP와 WTP사이에서 동작하면서 WAP에서의 상호 인증 및 채널 암호화를 담당하고 signText 함수는 WTLS가 제공하지 못하는 서명 기능을 지원함으로써 응용 레벨에서 부인 봉쇄 및 데이터의 무결성을 보장한다. 그리고 WIM은 사용자 비밀 데이터를 tamper-resistance 장치에 저장함으로 인한 정보의 불필요한 유출을 방지하고 사용자의 이동성(user mobility)을 지원해 준다. 그러나 이러한 보안 장치에도 불구하고 WAP에는 여전히 앞서 언급한 보안 홀(security hole)이 존재한다.

이와 연관해서 현재 WAP 보안에서 가장 시급한 문제는 WTLS에 존재하는 보안 약점의 보완과 WAP 무선 공개키 기반 구조의 확립이라 할 수 있다. WTLS의 보안 약점을 극복하기 위한 대안으로 WAP forum이 제안하는 WTLES과 달리 응용 레벨에서의 해결 방안을 생각해 볼 수 있으나 그것의 타당성 및 구체적인 방법에 대해서는 계속적으로 연구해야할 과제이다. WAP 무선 공개키 기반 구조는 보안 영역(security domain)의 모든 정보 보호 응용들을 지원하는 가장 중요한 요소라 할 수 있으므로 규격 제정이 느려진다면, CA 및 RA 그리고 WAP 응용 서비스가 서로 호환성이 없는 상태로 구현되어 보안 영역이 중첩됨으로써 향후 유무선이 완전한 통합 망으로 진화하는데 있어 커다란 걸림돌로 작용할 수도 있을 것이다.

참 고 문 헌

[1] Alan O. Freier, Philip Karlton, Paul C. Kocher, " The SSL Protocol, version 3.0", Netscape Communications Corp., Mar. 1996

[2] T. Dierks, C. Allen, "The TLS Protocol, version 1.0", IETF, RFC2246, Jan. 1999

[3] William Stallings, Cryptography and Network Security, Prentice Hall, 1999

[4] "Wireless Application Protocol Wireless Transport Layer Security Specification", WAP forum, Nov. 1999

[5] "Wireless Application Protocol Public Key Infrastructures Definition", WAP forum, Feb. 2000

[6] "Wireless Application Protocol Identity Module Specification", WAP forum, Nov. 1999

[7] "Wireless Application Protocol WMLScript Crypto Library Specification", WAP forum, Nov. 1999

[8] "Wireless Application Protocol Wireless Datagram Protocol Specification", WAP forum, Nov. 1999

[9] "Wireless Application Protocol Wireless Transaction Protocol Specification", WAP forum, Nov. 1999

[10] "Wireless Application Protocol Wireless Session Protocol Specification", WAP forum, Nov. 1999

[11] "Wireless Application Protocol Wireless Application Environment Specification", WAP forum, Nov. 1999

[12] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC press, 1996

[13] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987

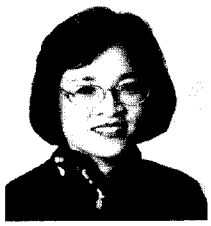
[14] Paul C. Kocher, Joshua Jaffe,

Benjamin jun, "Differential Power Analysis", Crypto'99, pp. 388-397, August 1999
[15] ISO/IEC 7816, Identification cards-Integrated circuit(s) cards with contacts
[16] PKCS#15 : Cryptographic Token Information Standard, version 1.0, RSA Laboratories, April 1999
[17] GSM11.11 : Digital cellular telecommunicaitons systems(Phase2 +); Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) Interface, ETSI
[18] "Wireless Application Protocol WAP Certificate and CRL Profiles Specification", WAP forum, May 2000
[19] "Wireless Application Protocol Transport Layer End-to-End Security Specification", WAP forum, Feb. 2000
[20] Markku-Juhani Saarinen, "Attacks Against the WAP WTLS Protocol", the proceedings of Communications and Multimedia security'99, Sept. 1999
(www.jyu.fi/~mjos/)

〈著者紹介〉

문 종 철 (Jong-cheol Moon)
1997년 2월 : 경북대학교 전자공학과 졸업
1999년 2월 : 경북대학교 전자공학과 석사
1999년 7월~현재 : 한국전자통신연구원 무선인터넷정보보호연구팀
〈관심분야〉 Cryptography, Internet Security, Smart card, Mobile computing

원 유 재 (Yoo-jae Won)
1985년 2월 : 충남대학교 계산통계학과 졸업
1987년 2월 : 충남대학교 계산통계학과 석사
1998년 8월 : 충남대학교 계산통계학과 박사
1987년 2월~현재 : 한국전자통신연구원 책임연구원 무선인터넷정보보호연구팀장
〈관심분야〉 Protocol Engineering, Mobile Computing, Internet Security, Multimedia Communication



조 현 숙 (Hyun-sook Cho)
1979년 : 전남대학교 수학과 졸업
1991년 : 충북대학교 전산학과 졸업
1999년 : 충북대학교 전산학과 박사수료
1982년~현재 : 한국전자통신연구원 책임연구원 정보보호기술연구본부장
〈관심분야〉 Network Security, Conditional Access, 인터넷 정보보호