情 報 保 護 學 會 誌
第 12 券 第 3 號, 2002. 6

무선 전자상거래를 위한 보안 기술

이 석 준*, 정 병 호**, 정 교 일***

요 약

CDMA2000, 무선랜 등의 무선 네트웍 접속 환경이 좋아지고, 무선 기기의 능력 역시 예전에 비하여 비약적으로 발전하면서 핸드폰이나 PDA와 같은 단말을 이용한 무선인터넷의 이용이 점점 늘어가고 있다. ADSL, 케이블 모뎀 등을 이용한 인터넷 환경이 발달하면서 인터넷을 이용한 전자상거래의 수요가 폭발적으로 증가했듯, 이제는 무선인터넷을 이용한 전자상거래의 수요가 매우 커질 것으로 보이며, 이동통신 업체와 금융권 등 무선 전자상거래에 관련이 있는 다양한 분야의 업체들이 이 부분에 주목을 하고 있다. 그러나 안전성과 편의성이 지원되지 않는 전자상거래 시스템은 아무런 의미가 없으며, 이는 곧, 무선 전자상거래를 위해서는 이를 위한 정보보호 기반 기술과 보안 프로토콜이 선행되어야 함을 뜻한다. 본 고에서는 무선전자상거래를 위한 기반 기술 및 프로토콜에 대해 살펴보고 국내외 동향을 알아보고자 한다.

1. 서 론

이동통신 기술이 14.4kbps내지는 56kbps의 저속망인 종전의 IS-95A/B 망에서 최고 144kbps까지 지원되는 CDMA2000-1x, HDR 혹은 그 이상의 속도가 지원될 IMT-2000 망으로 진화하면서 데이터, 멀티미디어 전송이 가능해짐에 따라 이를 이용한 무선 인터넷 시장이 매우 빠른 속도로 성장하고 있다. 인터넷에 연결된 컴퓨터만 있으면 전세계에 널리 퍼져 있는 수많은 정보를 접근할 수 있도록 해주는 인터넷의 특징에 언제 어디서나 상대방과 연결을 가능하게 해주는 무선 이동통신의 장점이 더해지는 만큼 무선인터넷 시장의 급성장은 당연한 결과라 할 수 있다.

한편, 유선인터넷에서와 같이 무선인터넷 상에서의 전자상거래 시장의 보편화도 무선인터넷의 보편화에 따른 자연스런 현상으로 볼 수 있다. 인터넷의 편리성과 효율성을 상거래에 접목, 경제적 효과를 극대화한 전자상거래는 무선인터넷에서 접근성이 훨씬 뛰어난 만큼 그 폭발력이 매우 크기 때문이다. 소비자 입장에선 여러 상품을 언제 어디서든 비교, 선택할 수 있는 장점이 있고, 이 곳 저 곳 돌아다니면서 물건을 고르는 불편과 비용을 덜 수 있는 장점이 있으며, 중간 유통과정이 생략되기 때문에 가격도 낮아진다.

그러나 전자상거래는 구매자와 판매자가 얼굴을 맞대고 사는 것이 아니며, 대금을 지불하는 방법 또한 실구매와는 다르기 때문에 그만큼 정보보호의 필요성이 크다고 볼 수 있다. 유선상에서의 전자상거래에서는 이를 위하여 안전한 지불 방법에 대한 연구가 많이 이루어져 있으며, 이를 이용하여 상대방에 대한 인증 및 구매 정보에 대한 위변조 방지를 위한 다양한 정보보호 프로토콜 및 기반 기술을 사용하고 있다. 무선인터넷 상에서의 전자상거래에서도 상황은 유선과 다르지 않다. 다만, 무선 이동통신의 데이터 전송 속도가 유선에 비해 저속이고, 패킷 전송 실패율이 크며, 그 데이터를 처리하고 가공하여 사용자와 직접 대화하는 무선 단말의 능력(화면크기, 메모리, 계산능력 등)이 일반 PC에 비해 현저히 떨어지는 만큼 이를 반영한 정보보호 기술의 적용은 무선 전자상거래에 있어 매우 필수적이라고 할 수 있다.

따라서 본 고에서는 무선 전자상거래에 필수적인 요소로 볼 수 있는 무선인터넷의 정보보호 기반 기

* 한국전자통신연구원 정보보호기반연구부 무선인터넷보안연구팀 연구원 (junny@etri.re.kr)
** 한국전자통신연구원 정보보호기반연구부 무선인터넷보안연구팀장 (cbh@etri.re.kr)
*** 한국전자통신연구원 정보보호기반연구부장 (kyoil@etri.re.kr)

술과 보안 프로토콜에 대해 살펴보고, 이를 어떻게 적용하고 있는지에 대한 국내외 동향을 서술한다.

II. 무선인터넷

앞서 설명한 무선인터넷 환경의 열악함은 정보보호 기술에 국한되는 것이 아니며, 이러한 제약 요소를 해결하기 위해 다양한 무선인터넷 규격이 제시되었다. 가장 널리 알려진 WAP(Wireless Application Protocol)[1]을 비롯하여 MME(Microsoft Mobile Explorer)[12], LEAP(Lightweight Efficient Application Protocol)[13], 일본의 i-mode[14] 등이 이러한 규격의 예로 볼 수 있다.

WAP은 에릭슨, 모토롤라, 노키아, Unwired Planet(현, Phone.com) 4개사가 포럼을 결성하여 만든 소형 무선 단말기를 위한 무선 인터넷 프로토콜이다. 현재 포럼에는 전세계 200 여개의 주요 단말기 제조업체, 이동통신 사업자들이 가입된 상태이다. WAP은 무선 단말기(client)와 인터넷 서버 사이에 프록시(proxy)역할을 하는 WAP 게이트웨이(gateway)를 두도록 하고 있다. 게이트웨이의 주요 역할은 WAP 프로토콜과 인터넷 TCP/IP 프로토콜을 중간에서 변환해 주는 것이다. 현재는 1.x 모델의 단점을 보완한 2.0 모델이 나와 있는 상태이다.

ME는 마이크로소프트사가 퀄컴과 제휴하여 제시한 방식으로 WAP 1.x 모델 방식과는 달리 유선 인터넷의 프로토콜 스택을 그대로 사용하는 방법이다. 하지만 무선 환경의 제약 때문에 기존 유선망의 콘텐츠를 수용할 수가 없어 m-HTML[16]이라는 HTML의 subset에 일부 기능을 추가한 마크업언어를 사용하여 서비스를 하고 있다. ME의 경우 기존 유선망 프로토콜 스택인 TCP/IP, HTTP를 그대로 사용하면서 보안방식도 기존 유선망 방식을 사용하려고 하였다. 하지만 ME 1.0에서는 SSL이 지원되지 않았으며, 최근 발표된 ME 3.0에서는 WTLS[3]와 SSL 3.0[20]을 지원한다.

LEAP은 WAP처럼 무선 응용에 적합하게 설계된, 그러나 WAP에서 생길 수 있는 특허 문제 등의 문제점을 제기한 대안 프로토콜이다. LEAP은 Efficient Short Remote Operation(ESRO), Efficient Mail Submission and Delivery (EMSD), Efficient Hyper Text Delivery (EHTD), Efficient Dictionary (E-DICT)로 구성되어 있다. ESRO는 신뢰적 비연결형 전송 계층이며, EMSD는 ESRO 상위 계층으로 메일전송 프로토콜인 SMTP를 최적화시킨 계층이다. EHTD는 EMSD와 함께 하이퍼텍스트 문서 전송에 최적화된 계층이며, E-DICT는 디렉토리 서비스를 위한 프로토콜 계층이다. 보안 기능은 ESRO 계층 위에 Secure Short Remote Operations (SSRO) 계층을 두어 제공한다.

i-mode는 1999년 일본의 NTT DoCoMo가 개발하여 폭발적인 인기를 얻은 패킷 기반의 무선인터넷 서비스이다. Compact HTML(c-HTML)[15]을 사용하며, 유선망과 무선망 사이에 게이트웨이를 두고 서비스를 한다. 초창기에는 게이트웨이와 웹서버 사이에서만 SSL방식의 보안을 적용하고 무선단말기와 게이트웨이 사이에는 보안을 적용하지 않았으나, 2000년 하반기 이후부터는 무선 구간까지 적용범위가 확대되었다.

III. 무선 전자상거래를 위한 보안 기술

유/무선인터넷에서는 전자상거래를 위한 다양한 서비스들이 존재한다. 그러나 이들의 안전성이 뒷받침이 되지 않으면 다양한 방식의 위협이 존재할 수 있으며, 따라서 필요한 서비스의 요구 사항을 그대로 지키면서도 그에 대한 안전성이 바탕이 되어야 한다.

전자상거래는 일반적인 상거래와는 분명히 다르며, 직접 대면하지 않고 거래가 이루어지므로 다음에 주의하여야 한다.

- 상대방의 신원의 확인 (사용자 인증)
- 제 3자에 의한 거래 정보의 위변조 방지 (메시지 무결성)
- 상대방에 의한 거래 정보의 위변조 방지 (부인 봉쇄)
- 제 3자에 거래 정보의 노출 방지 (메시지 기밀성)

사용자 인증은 주로 ID/password의 조합이나 인증서를 이용한 전자서명 등을 통해 이루어지며, 메시지 무결성은 메시지를 보낼 때 MAC(Message Authentication Code)이나 서명값을 포함하여 보냄으로써 얻을 수 있다. 부인 봉쇄는 전자 서명을 통해, 그리고 메시지 기밀성은 공개키/비밀키 암호화를 통해 이루어질 수 있다.

거래시에 이루어질 수 있는 다양한 위협 가능성에 대해서 위의 사항들과 함께 안전한 지불 시스템, 프

라이버시 보호를 위한 제도적 장치, 다양하고 편리한 배송 시스템 등의 사회적 여건이 구성된다면, 사용자들이 믿고 전자상거래를 할 수 있게 되는 것이다.

그러나 유선상에서 이루어지던 전자상거래가 무선 인터넷상에서도 정상적으로 이루어지기 위해서는 무선 환경의 특성을 고려한 보안 메커니즘의 적용이 필수적이라고 할 수 있다. 앞서 서론에서도 밝혔듯 무선 환경은 유선인터넷에 비해 다음 사항을 반영하여야 한다.

- 데이터 전송 속도 및 실패율을 고려하여 가급적 네트웍을 통해 전송되는 데이터가 적어야 한다.
- 단말기의 계산 능력이 떨어지므로 사용되는 공개키의 크기와 공개키 암호 알고리즘의 횟수를 최소화하여야 한다.
- 단말기 메모리의 크기가 작고 보안에 취약할 수 있으므로 가급적 단말기 메모리가 적게 사용되도록 하고, 스마트카드와 같은 장치를 이용하도록 한다.

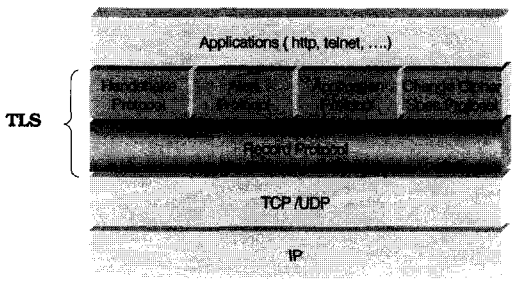
이 장에서는 전송계층 보안 프로토콜, 응용계층 보안프로토콜, WPKI, 스마트 카드 등에서 어떻게 이러한 점을 반영하여 보안 요구사항을 지키고 있는지를 알아보도록 하겠다.

1. 무선 전송계층 보안 프로토콜

인터넷에서 네트워크를 통해 전송되는 데이터에 대해서 정보보호 서비스가 필요한 경우 정보보호를 적용하는 것은 각각 그 계층별, 응용별로 방법이 다르다. 특히 다양한 응용 계층의 프로토콜의 보안 요구 사항을 만족시키기 위하여 각 응용 프로토콜 별로 각각의 정보보호 프로토콜을 제작하면, 그 응용에서 필요한 요구 사항에 대해 가급적 모든 조건을 만족시킬 수 있다는 장점은 있지만, 범용성 측면에서 매우 불합리한 구조를 지니게 된다. 따라서 각 응용 프로토콜의 요구사항은 모두 만족시키지 못하더라도, 전체적으로 모든 응용에 대해서 통일된 보안 서비스를 제공할 수 있는 역할을 수행하는 전송계층 보안프로토콜이 필요하다.

전송계층 보안프로토콜은 기밀성, 사용자인증, 무결성을 제공하지만, 부인 봉쇄는 제공하지 않는다. 부인 봉쇄는 보통 응용에서 이 서비스가 필요한 부분만 전자 서명을 함으로써 달성되는데, 그 이유는 전자 서명이 공개키 연산을 수행하여 지나치게 비효율적일 뿐더러, 부인 봉쇄는 대체로 메시지 기반의 응용에서 특수한 상황에서 필요한 보안 서비스이기 때문이다.

유선상에서의 전송계층 보안프로토콜인 TLS[17]의 구성은 그림 1과 같다. 여기서 Handshake 프로토콜은 상대방에 대한 인증 및 보안 세션을 설정하기 위하여 필요한 정보를 교환하는데 사용한다. 이때, 서버와 클라이언트는 프로토콜 버전과 대칭키 암호 알고리즘을 결정하고, 대칭키를 생성한다. 그리고 인증서 교환을 통하여 상호 인증을 수행한다. Record 프로토콜은 핸드쉐이크 이후 서버와 클라이언트가 합의한 보안 설정 값을 바탕으로 데이터를 압축, 인증코드를 첨가한 후 암호화하여 전송하는 작업과 수신한 데이터를 복호화하고 인증코드값을 검사하고 데이터를 해제하는 기능을 한다. Alert 프로토콜은 통신 중에 발생한 문제에 대하여 알려주는 기능을 한다. Change Cipher Spec 프로토콜은 데이터가 보안 설정 값을 바탕으로 통신을 시작함을 알려주는 기능을 한다.

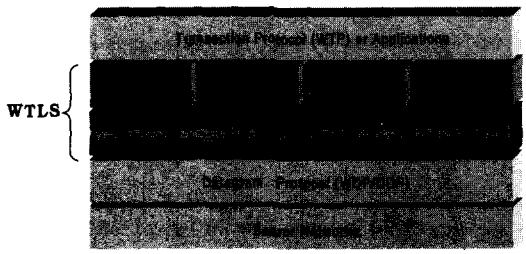


〔그림 1〕 TLS 프로토콜

1.1 WTLS (Wireless Transport Layer Security)

유선상에서 전자상거래를 위해 널리 사용되었던 SSL[20]과 이를 약간 개량하여 IETF에서 RFC로 상정한 TLS[17]는 유선 전송계층 보안프로토콜의 사실상의 표준이라고 할 수 있다. 그러나 WAP Forum에서 WAP 1.x 프로토콜 스택을 사용할 경우 SSL/TLS를 그대로 사용하지 못하여, 이를 무선 환경에 맞도록 수정한 것이 WTLS[3] 이다.

WTLS 프로토콜은 WTP(Wireless Transaction Protocol)[5]과 WDP(Wireless Datagram Protocol)[6] Layer 사이에 위치하며, 그림 2와 같은 구성을 가진다.



〔그림 2〕 WTLS 프로토콜

WTLS는 프로토콜 구성이나 동작 방법이 SSL/TLS과 거의 유사하지만 일부 구분되는 점이 있는데 이는 다음과 같다.

- 전송계층이 신뢰성이 보장되는 TCP가 아닌 WDP/UDP이다. 따라서 신뢰성을 보장하는 매커니즘이 포함되어 있어야 하며, 이를 위하여 sequence number를 사용한다.
- 무선상에서 전송되는 데이터의 수가 최소화되어야 한다. 따라서 핸드쉐이크 방식에 기존의 Full/Abbreviated 핸드쉐이크 외에 Optimized/Shared-Secret 핸드쉐이크가 추가되었으며, 핸드쉐이크의 횟수를 최소화하기 위해 키 재생성도 가능하도록 하였다.
- 암호 연산의 부담을 줄이기 위해 *master secret*과 random number의 크기를 줄였으며, PRF (Pseudo Random Function) 함수 수행시 하나의 해쉬함수를 사용하도록 하였다. 그리고 보안 강도에 비해 키의 크기가 작은 ECC 알고리즘을 추가하였다.
- X.509 인증서의 처리 부담을 줄이기 위해 서버 인증서로 사용될 수 있는 WTLS 인증서와 X9.68 인증서 방식을 추가하였으며, 단말 인증서를 무선상으로 직접 전송할 때 생기는 부담을 최소화하기 위한 URL 인증서 방식도 추가하였다.

1.2 TLS (Transport Layer Security) for wireless e

앞 절에서 밝힌바와 같이 WTLS는 유선인터넷을 위한 전송계층 보안프로토콜의 표준격인 SSL/TLS와는 여러 가지 차이점을 가지고 있으며, 무선환경을 충분히 고려하여 만든 규격인 만큼 SSL/TLS에 비해 여러 가지 기능이 최적화되었거나 추가되어 있다. 그러나 무선인터넷의 특성을 반영했음에도, WTLS는 하위 프로토콜이 WDP이고 SSL/TLS와 호환이 되지 않아 휴대단말과 웹 서버사이에 단대단 보안을 제공하지 못한다는 약점을 지니고 있어 표준화에 큰 걸림돌이 되고 있다.

따라서 2000년 8월 IETF meeting에서는 WAP Forum Security Group의 의장을 맡고 있는 Tim Wright는 IETF와의 공동작업을 위한 발표를 하여 다음 사항에 대해 고려하여 TLS 1.1을 만들 것을 제안하였다.

- 인증서는 X.509에 따름
- WIM의 사용
- ECC와 RC5의 사용
- 클라이언트의 URL 인증서 사용
- 핸드쉐이크시 단말은 최상위 인증기관에 대한 정보를 가지고 서버에 대해 이 인증기관의 인증서는 요구하지 않음
- Datagram 지원과 WTLS 인증서는 필요하지 않을 수 있음

이를 위하여 IETF에서 TLS 1.0에 무선환경을 고려한 약간의 수정 및 차기 버전(TLS 1.1)에 대한 요구 사항을 정리할 것을 요구하였으며, 이를 위해 2000년 11월 Certicom의 Simon Blake-Wilson과 RSA Security사의 Magnum Nystrom은 무선 환경을 고려한 TLS 확장 규격[19]을 IETF TLS working group에 Internet Draft로 제안하였고, 역시 Internet Draft로 올라와 있는 TLS v1.0 revision[18]에서는 이 확장 규격을 추후 지원할 수 있음을 명시하고 있다. 이 확장 규격이 추구하는 내용 중 무선을 고려한 내용은 다음과 같다.

- 최대 record size에 대한 협상 기능
- 단말의 URL 인증서 사용
- 단말이 소유한 root CA 키를 서버에 알릴 수 있는 기능
- 크기를 줄인 MAC의 사용 기능
- CRL을 대신하여 OCSP 사용

2. 무선 응용계층 보안 프로토콜

전송계층 보안프로토콜을 사용하는 경우 전송계층 전체에 대한 보안이 설정된다. 이러한 경우에 전송되는 모든 데이터가 암호화되기 때문에 보안 적용이 필요하지 않은 데이터까지 암호화되어 불필요한 오버헤드(overhead)가 발생할 수 있다. 또한, 트랜

잭션 단위의 선택적 암호화/전자서명의 기능이 필요한 응용도 있다. WAP Forum에서는 이를 위하여 WMLScript[2]를 이용하여 응용계층에서 보안 서비스를 달성할 수 있도록 하였다.

최근 WAP 포럼에서는 전자서명과 관련된 signText 응용 프로그램 인터페이스(API)만이 표준화 되어있던 WMLScript Crypto 라이브러리[4]를 확장하여 사용하는 방법이 논의되고 있다. 그 중에는 Vodafone, Telstra, Certicom이 제안한 encryptText, encrypt[8]와 veriSign에서 제안한 initContext, initContext-Final, closeContext[9] API 등이 WAP security group의 draft 상태로 논의가 진행중이다.

2.1 WMLScript를 이용한 서명

WAP Forum에서 내놓은 WMLScript Crypto API 규격에는 현재까지 전자서명에 대한 부분만이 정해져 있다. signText라는 함수로 정의된 전자 서명을 이용하여 서명된 메시지에 대한 인증 및 부인봉쇄 서비스가 가능해진다.

```
signedString = Crypto.signText
        (stringToSign,
         option,
         keyIdType,
         keyId)
```

이 함수는 stringToSign이라는 서명하고자 하는 메시지에 대해 전자 서명을 수행하며, user는 전자 서명 과정을 취소하거나 승인할 수 있다. 서명을 위해서는 반드시 비밀키에 대한 인증 정보를 user에게 묻도록 한다. 서명에 대한 결과를 base64 방식의 인코딩 절차를 거쳐 signedString으로 내보낸다. options는 서명 메시지 생성시 메시지나 인증서를 포함할지 등에 대한 옵션값이며, keyIdType은 keyId값의 종류, keyId값은 키를 identify하는 값으로 주로 공개키의 해쉬값을 사용한다.

사용가능한 서명 알고리즘으로는 RSA 와 ECDSA 이며, 단말은 둘 중 하나를 반드시 지원해야 한다.

2.2 WMLScript를 이용한 암복호화 솔루션 I (일회성 암화 방식) - vodafone, telstar, certicom

2001년 4월 Vodafone, Telstra, Certicom은 기존의 WMLScript Crypto 라이브러리를 확장하여 단말에서 일회성 암호화가 가능하도록 encrypt, encryptText라는 함수에 대한 규격을 WAP Forum에 draft[7]로 제안하였다.

응용 계층에서의 기밀성을 보장하기 위해 만든 이 함수들은 메시지를 보호하기 위해 랜덤하게 만든 대칭키를 사용하여 암호화하며, 이 대칭키는 서버의 공개키를 이용하여 다시 보호하도록 한다. 서버는 이 과정을 역으로 하여 메시지를 복호화할 수 있게 된다. encrypt함수는 사용자 인터페이스가 없는 함수이며, encryptText는 사용자 인터페이스를 제공하고 함수 안에서 encrypt를 호출하는 방식을 사용하고 있다.

```
WapEnvelopedData = Crypto.encrypt
        (flag,
         dataToEncrypt,
         recipientPublicKey,
         keyManagementAlgorithm,
         contentEncryptionAlgorithms,
         rid_type,
         rid)
```

이 함수는 dataToEncrypt의 내용을 암호화하여 WapEnvelopedData라는 데이터 형식으로 만들어 이를 base64 인코딩한 결과를 내보내도록 한다. flag는 dataToEncrypt의 인코딩 방식이며, recipientPublicKey는 대칭키 형식의 암호화 키를 보호할 공개키, keyManagementAlgorithm은 공개키 암호 알고리즘, contentEncryption Algorithm은 대칭키 암호 알고리즘의 종류이다. rid_type는 rid의 종류를 나타내며, rid는 recipientPublicKey의 identifier이다.

```
WapEnvelopedData =
        Crypto.encryptText(
        Prompt,
        DefaultText,
        RecipientCertChain,
        KeyManagementAlgorithm,
        ContentEncryptionAlgorithms)
```

이 함수는 사용자로부터 입력을 받은 내용을 서버에게 암호화하여 보내는 역할을 수행한다. prompt는 사용자에게 입력을 받기 앞서 보여줄 메시지이며,

DefaultText는 사용자가 입력할 내용의 default 값을 나타낸다. RecipientCertChain은 이 메시지를 받을 이의 공개키 인증서 체인이며, KeyManagement-Algorithm과 ContentEncryptionAlgorithm은 앞의 Crypto.encrypt 함수와 같다.

이 두 함수에서 사용가능한 공개키 암호 알고리즘은 Diffie-Hellman, ECC-DH, RSA이며, 대칭키 암호 알고리즘은 Triple-DES와 RC5로 되어 있으나 현재 RC5는 Key Wrap Algorithm에 대한 정의가 내려져 있지 않아 Triple-DES만 사용가능한 상태이다.

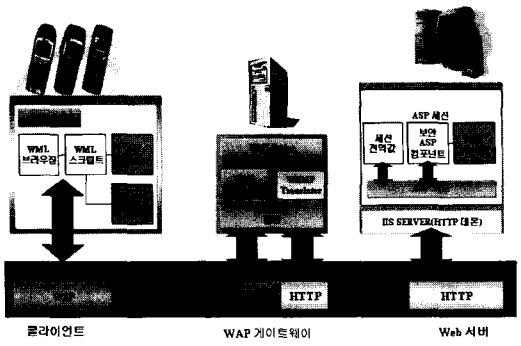
2.3 WMLScript를 이용한 암복호화 솔루션 II (secure session을 맺는 방식)

앞서 2.2에서 설명한 암복호화 솔루션은 현재 WAP Forum에서 Draft 상태로 되어 있으며 계속 논의중임에도 불구하고 일회성 암호화로 지원이 된다는 단점을 가지고 있다. 즉, 단말과 서버 사이에 어떤 보안 세션을 미리 맺은 상태가 아니므로, 암호화를 해야 할 일이 있으면 그 때마다 임시 대칭키를 생성하고, 그 대칭키 역시 매번 공개키로 암호화해서 보내주어야 한다는 의미이다. 이는 메시지 기밀성이 자주 일어나지 않는 경우에서는 유용할 수 있으나, 보호받아야 하는 트랜잭션이 어떤 한 세션에서 여러번 일어나야 할 경우는 미리 공개키를 이용한 보안 세션을 맺고(대칭키 공유), 암호화가 필요할 때 대칭키 암호화만 수행하도록 하는 방법이 유용할 수 있다.

이를 위하여 veriSign과 같은 업체에서 WAP Forum에 CR(Change Request)[9]를 제출하고 있으며, 국내에서는 ETRI에서 WTLS library를 응용 계층에서 활용한 솔루션을 설계, 구현하였다.

2.3.1 WMLScript를 이용한 암복호화 설계 원리

그림 3과 같이 ETRI에서 설계한 방식은 전송계층에서의 보안프로토콜과 유사하게 먼저 단말과 웹 서버 사이에 보안 세션을 맺기 위한 핸드쉐이크 절차를 거치도록 하는 것이다. 다만 차이점은 이를 수행하는 계층이 응용계층이며, 세션을 맺는 주체가 단말 대 WAP 게이트웨이가 아닌 단말 대 웹 서버라는 점이다. 그러므로 WTLS의 약점으로 지적되는 웹 서버와 직접 단대단 보안 문제도 자연스럽게 해결될 수 있다.



[그림 3] WMLScript를 이용한 단대단 보안 모델

설계에 대한 기본 원리는 다음과 같다.

- 단말
  - 확장될 WMLSCript 라이브러리는 Crypto 라이브러리이며 기존의 전자 서명을 위한 SignText함수에 HandShake, Encrypt, Decrypt 함수를 추가함
  - 클라이언트에서 WTLS 구현시에 사용된 보안 라이브러리를 그대로 이용함
- WAP 게이트웨이
  - 서버에서 보낼 새로운 WMLScript 함수를 컴파일할 수 있도록 컴파일러 수정
- 웹 서버
  - Windows IIS 서버 기반
  - ASP 세션 관리 매커니즘을 보안 세션 관리 매커니즘으로 재활용
  - WTLS 구현시 사용된 보안 라이브러리를 컴포넌트로 포팅하여 재사용

2.3.2 WMLScript를 이용한 암복호화 구현

단말과 웹 서버간 단대단 보안을 제공하기 위해서는 단말, WAP 게이트웨이 및 웹 서버 모두에 특수한 기능을 추가하여야 한다. 먼저 WMLScript의 라이브러리를 추가하였으므로 이 라이브러리를 인식하여 바이트코드 형태로 컴파일 할 수 있는 컴파일러의 기능을 확장하여야한다. 그리고, 단말에서도 마찬가지로 확장된 라이브러리를 인식할 수 있도록 스크립트 인터프리트 기능을 확장하여야 한다. 그리고, 웹 서버도 역시 클라이언트와 보안 정보를 교환하고 보안을 적용시키기 위한 기능이 추가되어야 한다. 보안 관련 모듈들을 ASP 컴포넌트로 만들면, 무선 웹 개발자는 컴포넌트를 설치하고 컴포넌트를

사용함으로써 안전한 무선 웹 사이트를 만들 수 있다.

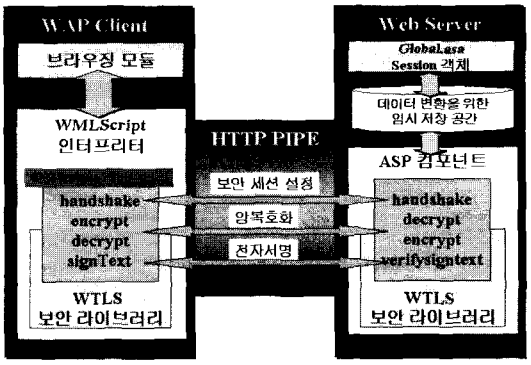
클라이언트의 보안 라이브러리는 서버의 보안 라이브러리와 상호 작용하여 보안 세션을 설정, 종료하고 보안 정보를 적용하기도 한다. 먼저 보안 세션을 설정하기 위해서는 핸드쉐이크를 수행한다. 핸드쉐이크 수행시에는 보안 협상 정보들이 양자간에 교환되어야 한다. 이 메시지들은 HTTP-파이프(WSP와 HTTP 프로토콜)를 사용하여 신뢰성 있게 전달된다. 이때 사용되는 핸드쉐이크 메커니즘과 전달되는 메시지의 형식은 WTLS의 메카니즘과 메시지 형식을 그대로 사용한다. 이렇게 협상된 보안 정보들은 각각의 보안 관리 영역에 보관된다. 클라이언트는 보안 관리 영역을 위한 전역 객체에 저장될 것이며, 웹 서버의 경우에는 ASP의 세션 관리 메커니즘을 사용하여 관리하고자 한다. ASP에는 Global.asa라는 파일에 설정된 객체들을 하나의 세션 마다 독립적으로 관리해주는 메커니즘이 있다. 이 메커니즘에 따라 Global.asa에 보안 관련 전역 값들을 추가하고 웹 세션 관리 메커니즘을 그대로 보안 세션 관리 메커니즘으로 사용하였다.

이러한 과정을 통하여 만든 단대단 보안 라이브러리 API를 표 2에 나타내었다.

〔표 1〕 단대단 보안 API

단말	Bool handshake(String handshakeURL, String nextpageURL)
	String signText(string ToSign, int *options*, *int KeyidType*, *String Keyid*)
	String encrypt(string ToEncrypt)
	String decrypt(string ToDecrypt)
서버	HRESULT handshake()
	HRESULT verifysigntext(BSTR signin, BSTR indata, BSTR url)
	HRESULT encrypt(BSTR plaintext, BSTR *rplaintext)
	HRESULT decrypt(BSTR plaintext, BSTR *rciphertext)

위의 라이브러리를 통하여 보안 세션을 맺고 암복호화를 수행하는 동작 원리는 그림 4와 같다. 단말이 handshake 스크립트 API를 통하여 웹서버의 ASP를 참조할 때, 서버에서는 Crypto ASP 컴포넌트가 생성되고, Crypto 객체의 hanshake API가 호출되면서 핸드쉐이크가 수행된다.



〔그림 4〕 E2E Crypto 라이브러리 동작 모델

이 과정에서 서버의 global.asa에 설정된 세션 객체는 WTLS 라이브러리를 사용하면서 생성되는 보안 세션 정보를 임시 저장 공간을 통하여 객체 내부에 저장한다. 단말의 경우는 프로세스가 생성하는 메모리 영역에 보안 세션 정보가 저장된다. 세션 관리 및 유지는 IIS 서버가 제공하는 ASP 세션 메커니즘을 그대로 사용한다. 단말은 서버가 설정한 세션 ID 사용이 가능하도록 쿠키값을 유지 할 수 있어야 한다. 암복호화는 보안 세션 정보를 바탕으로 이루어지며, 전자 서명의 경우 서명용 인증서를 이용하여 하도록 하였고, 서명과 암호화를 동시에 수행할 수도 있도록 하였다.

ETRI에서 구현한 방식은 WTLS 라이브러리를 그대로 재활용하여 사용할 수 있도록 되어 있으므로 핸드쉐이크시 사용되는 공개키 암호 알고리즘이나 메시지 암호화를 위한 대칭키 암호 알고리즘, 사용하는 인증서 종류, 스마트 카드 지원 여부 등의 특성을 WTLS로부터 그대로 물려받는다.

3. WPKI (Wireless Public Key Infrastructure)

앞에서 설명하고 있는 전송/응용계층 보안프로토콜에서는 공개키 암호 알고리즘의 사용이 필수적이다. 일부에서는 패스워드를 이용한 인증 및 키교환 방식에 대한 연구[23-26]가 이루어지고 있기는 하나 실용화 단계에는 머무르지 못하고 있는 실정이다. 따라서 공개키 암호 알고리즘의 효과적인 운영을 위한 PKI(공개키 기반구조, Public Key Infrastructure)의 구축은 반드시 이루어져야 한다.

현재 유선인터넷 상에서의 PKI 구축은 빠르게

이루어져 있어 증권, 금융, 쇼핑 등의 전자 상거래가 이루어질 수 있는 핵심 분야에 대한 공인인증기관이 지정되어 있고, 이를 통한 일부 상용 서비스가 이루어지고 있다.

그러나, 무선 환경의 제약은 유선인터넷 상에서 구축되어 있는 PKI를 무선인터넷에 그대로 적용하는 것을 곤란하게 한다. 그러므로 무선인터넷으로 생길 수 있는 여러 상황을 반영한 WPKI 규격이 만들어져야 하는 것이다.

현재 WAP Forum에서는 이와 관련하여 다음과 같은 규격들이 정의되어 있다.

- WTLS (WTLS 인증서가 정의되어 있음)[3]
- WAP Public Key Infrastructure Definition[10]
- WAP Certificate and CRL Profile[11]

우리 나라에서는 ETRI와 KISA, 보안 관련 업체들이 중심이 되어 만든 인터넷보안기술포럼에서 WPKI 관련 표준을 제정하고 있으며, 올해 4월 다음과 같은 규격을 발표하였다.

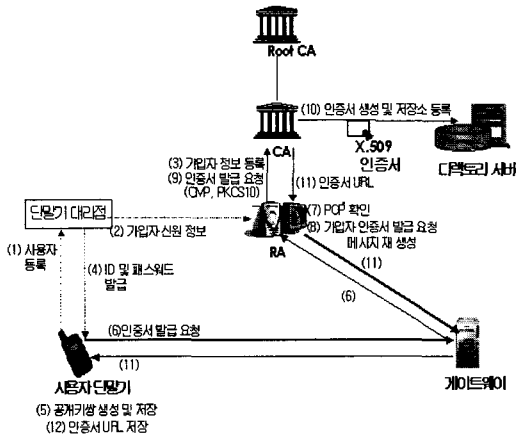
- 무선 전자서명 인증서 프로파일 표준[27]
- 무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준[28]
- 무선 WTLS 인증서 프로파일 표준[29]
- 무선 전자서명 알고리즘 표준[30]
- 무선 키분배 알고리즘 표준[31]
- 무선 인증서 요청형식 표준[32]

3.1 WPKI 구성

무선 PKI 시스템은 유선 PKI 환경과 마찬가지로 다음과 같은 구성 요소를 가지고 있으며, 이외에 WAP 환경의 경우 무선 PKI 서비스가 보다 효과적으로 가능하도록 하기위해 실제 무선 PKI 서비스의 일부 구성 요소로 WAP 게이트웨이 서버가 포함된다.

- CA 서버 시스템 : 인증서 발급, 관리
- RA 서버 시스템 : 인증서 발급, 관리 요청 중계
- 클라이언트 시스템 : 인증서 발급, 관리 요청
- 디렉토리 서버 시스템 : CA가 발행한 인증서 정보를 저장, 관리

그림 5는 무선 PKI 시스템의 구성과 사용자의 등록에서 인증서의 요청 및 발급에 이르는 일련의 무선 PKI 시스템 운용 절차에 대한 설명이다.



〔그림 5〕 무선 PKI 시스템 구성

3.2 WPKI 인증서 발급 절차

WPKI 인증서 발급 절차는 발급받는 WPKI 클라이언트가 단말인 경우 발급정보를 보호하고 POP (Proof Of Possession)의 확인하는 절차에 초점이 맞춰진다.

인증서 발급 절차는 WAP Forum에서 제시하고 있는 것과 국내 표준과 다르며, 국내 표준은 발급정보 보호 및 POP 확인을 WTLS 대신 일회성 Passwordbased MAC과 signText를 이용하도록 하였다. 국내 표준상에서 제시된 전자서명 및 키분배용 인증서 요청 형식 구조[32]는 다음과 같다.

- 단말 ← CA(RA) : nonce 전달
- 단말 : nonce를 바탕으로 다음값 계산
  nonce를 $SK_{\text{키분배}}$로 서명, $SignValue_{\text{키분배}}$ 생성
  $M = type|PK|ID|PK_{\text{키분배}}|SignValue_{\text{키분배}}|nonce$
  $N = Password$
  $SignedContent = signText(M|H(M,N),1,0,"\ ")$
- 단말 → CA(RA) : SignedContent 전달
- CA : $SignedContent$에서 M 추출
  M에서 PK, ID, $PK_{\text{키분배}}$, $SignValue_{\text{키분배}}$ 추출
  $SignedContent$를 검증하여 서명용 POP 확인
  $SignValue_{\text{키분배}}$를 검증하여 키분배 POP 확인
  DB상의 ID, Password로부터 N 구성
  M, N을 해쉬한 값과 $SignedContent$에 있는

$H(M,N)$을 비교하여 사용자 인증

type : 관리 형식의 type string 값 (100)
PK : 가입자의 서명용 공개키
$PK_{키분배}$: 가입자의 키분배용 공개키
$SK_{키분배}$: 가입자의 키분배용 비밀키
ID : 가입자의 참조번호
Password : 가입자의 인가코드
$SignValue_{키분배}$: 키분배용 POP 확인을 위해 nonce값에 키분배용 개인키로 서명한 값
nonce : 서버가 생성한 UTC time

이에 대한 결과 메시지는 사용자 인증 및 POP 확인에 성공한 경우, MIME Type을 application/vnd.wap.cert-response로 하고 실제 인증서 정보를 base64 인코딩하여 보내도록 한다. 인증서 내용은 전자 서명용 인증서, 키분배용 인증서를 모두 포함할 수 있으며, URL 인증서와 X.509 인증서의 형식이 가능하다.

인증서의 공개키 암호 알고리즘은 ECDH, ECDSA, RSA 등이 가능하며, 실제 키길이나 알고리즘에 관련된 표준은 무선 전자서명 알고리즘 표준이나 무선 키분배 알고리즘 표준 등을 참조한다. signText 함수는 앞서 2.1에서 설명한 함수와 동일하며 전자서명용 인증서 혹은 키분배용 인증서만을 발급받을 때의 인증서 요청형식 구조는 좀 더 간단해지며 여기서는 생략하고자 한다.

4. 스마트 카드

스마트카드는 마이크로 프로세서와 메모리를 내장하고 있어 카드 내에서 정보의 저장과 처리가 가능한 카드를 말한다.

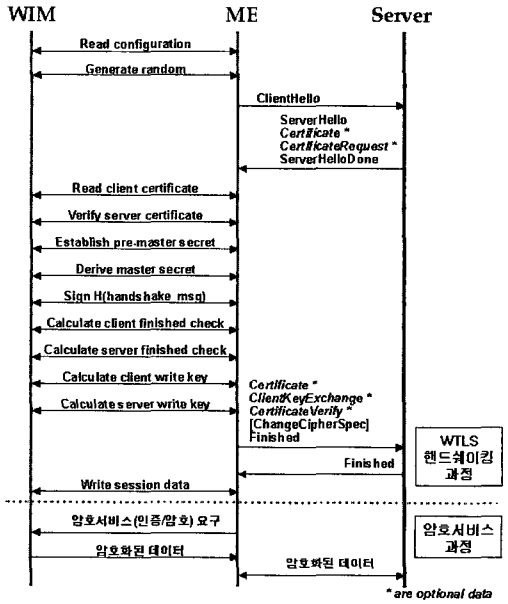
RSA와 같은 암호 알고리즘을 하드웨어적으로 구현한 코프로세서 등이 장착된 스마트카드가 나오면서 단말의 부족한 연산 능력을 스마트카드가 보조해 주는 것이 가능해졌다. 또한 인증서나 비밀키 등과 같이 중요한 정보를 단말이 아닌 스마트카드에 저장할 수 있으며, 이러한 점은 무선 전자상거래의 보안 요소로 스마트카드가 사용되어야 함을 뜻하게 된다.

WAP Forum에서도 이와 같은 상황을 반영하여 WIM(WAP Identity Module) 규격[7]을 발표하였으며, WIM을 이용하여 WTLS, signText와 같은 보안 프로토콜에서 서명, 인증서 검증, 해쉬 함수 등에 활용할 수 있도록 하였다. 또한 3세대 이동통신 표준 단체인 3GPP[22]에서도 USIM(Universal Subscriber Identity Module) 규격[23]을 제안한 바 있다.

4.1 WIM (WAP Identity Module)

WIM[7]은 WAP Forum에서 WTLS, 응용계층 보안 등에 보다 더 안전한 보안 서비스를 제공하기 위해 만든 스마트 카드 응용 규격이다. 즉, WTLS에 WIM이 같이 사용되는 경우, WIM에서는 random number의 생성, 서버인증서 검증, 단말인증서 저장, 세션키 생성 및 암호화, WTLS 핸드쉐이크 검증 등 대부분의 암호 서비스를 처리하도록 한다.

WTLS를 이용한 핸드쉐이크 및 보안 세션 설립시에 WIM과 어떻게 작동을 하는지에 대해 그림 6에서 설명하고 있다. 단말의 WTLS는 WAP 게이트웨이와 공유하기 위해 생성하는 premaster secret과 이를 이용하여 만든 master secret을 알지 못하며, 이 값은 오직 WIM 카드 내에서만 존재한다. WTLS는 그 master secret을 이용하여 만든 임시 암호화키와 MAC 키, IV값을 WIM으로부터 전달받아 실제 서버로 메시지를 암호화하여 전송할 때 사용한다.



〔그림 6〕 WIM Operation in WTLS

이 외에도 signText를 비롯한 여러 응용에서 WIM을 사용할 수 있으며, WIM 규격에서 응용이 접근할 수 있는 프리미티브와 APDU 등을 정의해 놓았다. ETRI가 만든 응용계층 보안프로토콜에서도 WIM을 사용하여 핸드쉐이킹을 할 수 있다.

4.2 USIM (Universal Subscriber Identity Module)

USIM은 인증 및 키일치를 통하여 생성된 암호키를 바탕으로 사용자 데이터에 대한 암호 및 인증 서비스를 제공한다.

USIM은 다음과 같은 알고리즘을 포함해야 한다.

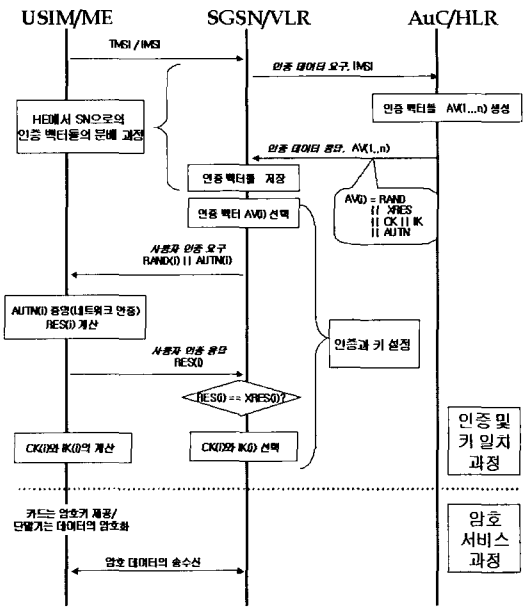
- f0 : 난수 발생 알고리즘
- f1 : 네트워 인증을 위한 XMAC 알고리즘
- f1* : 재동기화 인증함수
- f2 : RES(user RESponse) 생성을 위한 사용자 인증 함수
- f3 : 암호화키 CK를 생성하는 함수
- f4 : 무결성 검증 키를 생성하는 함수

그리고 다음의 함수를 옵션으로 가지도록 한다.

- f5 : 익명키 AK 생성 함수
- f5* : 재동기화를 위한 익명키 유도 함수
- c2, c3 : 2세대 SIM 카드와의 호환성 제공을 위한 함수

USIM은 TMSI(Temporary Mobile Subscriber Identity)나 IMSI(International Mobile Subscriber Identity)를 VLR에게 보내면 VLR는 다시 이를 인증 데이터 요구 메시지와 함께 인증 센터에게 보낸다. 응답으로 받은 인증 벡터를 바탕으로 인증 토큰을 단말에 보내면 USIM을 이용하여 인증 절차와 키 생성을 한다. VLR은 USIM이 보내는 RES와 XRES를 비교하여 단말을 인증하고 키 생성을 하여 단말과 키 공유를 하게 된다. 실제 키를 사용하는 것은 단말과 RNC에 있는 동기식 스트림 암호 알고리즘이며, USIM은 인증과 키 공유를 담당하는 것이다.

이 과정은 그림 7에서 나타내었다.



〔그림 7〕 USIM에서의 휴대 단말 암호 서비스

Ⅳ. 무선 전자상거래 보안 기술 국내외 동향

초기 무선인터넷 서비스가 출현할 당시에는 텍스트 기반의 저속 네트워 환경이었으며 단말기에서 공개키 암호 알고리즘을 수행시키는 것 자체가 부담이었으나 현재 2.5세대 이동통신 서비스가 제공되면서 무선인터넷 환경이 점점 멀티미디어, 대용량 데이터, 보다 빠른 처리 속도로 발전하고 있다. 무선인터넷 환경이 바뀐다는 것은 곧 무선 전자상거래를 위한 환경도 바뀐다는 것을 의미하며, 또한 기반이 되는 정보보호 알고리즘 혹은 프로토콜의 규격이 수정될 수 있다.

WAP Forum에서도 기존의 1.x대 프로토콜에 이어 유선인터넷에서 사용하던 TCP/IP 프로토콜을 활용하는 2.x대 프로토콜 스택을 2001년 중반에 발표했으며, 계속된 규격 업데이트 중[1]에 있다. 여기에서는 전송계층 보안프로토콜로 WTLS를 사용하던 것을 TLS 터널링을 이용하도록 하고, TLS를 보다 더 효율적으로 사용할 Profile을 정의하는 한편, WPKI 등 정보보호에 관련된 규격을 계속 검토 및 수정 작업을 하고 있다.

이와 더불어 IETF TLS working group에서는 TLS 1.0 revision이 이루어지고 있으며, WAP Forum과의 공동 작업을 통한 TLS 확장이 진행 중에 있다.

또한 무선 뱅킹, 증권, 의료 서비스 등 다양한 응용이 WIM, USIM 카드의 활용을 요구하고, 이러한 요구를 지원하기 위해 필수적인 하드웨어와 카드 운영체제 등의 기술이 발전함에 따라, 이들 응용들을 지원할 수 있는 기능이 추가되거나 WIM과 USIM의 통합 가능성이 논의되고 있다.

이에 발 맞추어 각국의 많은 보안 업체와 이동 통신, 단말기, 스마트카드 관련 업체이 WPKI 기반의 스마트카드 시장을 선점하기 위한 다양한 노력을 기울이고 있다. 핀란드의 소네라, 노르웨이의 텔레노, 스페인의 보다폰 등과 같은 통신 업체을 중심으로 주도권 싸움이 치열할 것으로 보인다.

한편 우리 나라는 무선 전자상거래를 위한 보안 기술 및 프로토콜에 대한 표준 정의 및 구현에 있어 세계적으로 매우 발빠른 행보를 보이고 있다. 인터넷보안기술포럼과 같은 민간 포럼에서는 무선 PKI에 관련한 여러 규격을 표준으로 상정하였으며, 각 공인 인증 솔루션 업체들은 이동 통신 업체와 손을 잡고 무선 인증 시장 확산을 위한 노력 중에 있다.

이들 대부분의 업체들은 공개키 암호 알고리즘으로 RSA보다는 같은 안전성을 가질 때 키길이가 보다 짧고 속도가 빠른 ECC을 채택하고 있는 것이 특징이다.

이에 앞서 작년 10월 ETRI에서는 WIM 카드에 대한 기술 개발에 성공하였고, 응용 계층에서 보안 세션을 맺는 단대단 보안 기술을 개발하였다. 이들을 이미 개발한 WPKI와 연동하여, 무선 단말이 전자 서명용, 키 분배용 인증서를 발급받아 WIM 카드에 저장한 후, WIM 카드를 이용하여 응용 계층에서 보안 세션을 맺고 암복호화 및 전자서명을 이용한 무선 인터넷 뱅킹을 시연하는데 성공하였다. 무선 전자상거래를 위해 필요한 보안 기술을 모두 개발하고 이들을 연동하여 종합적으로 운용할 수 있음을 보인 것이다.

현재까지는 WPKI를 기반으로 한 서비스는 거의 전무한 실정이지만, LG 텔레콤과 한국정보인증 등이 WPKI 기반의 무선 전자상거래 서비스를 하겠다고 밝힌바 있고, SK 텔레콤과 KTF 등에서도 시범 서비스에 들어갈 것으로 보인다.

V. 결 론

본 고에서는 무선 전자상거래에 필요한 관련 보안 기술 및 정보보호 프로토콜 등에 대해서 알아보았다. 이들 기술은 독자적으로 동작할 수 없으며, 무선 전송계층 보안프로토콜, 응용계층 보안프로토콜, WPKI, 스마트 카드 기술들이 서로 유기적으로 결합할 때 인증, 기밀성, 무결성, 부인 봉쇄와 같은 다양한 정보보호 서비스가 효과적으로 구성되어 안전한 무선 전자상거래가 이루어질 수 있다.

CDMA로 대변되는 이동통신 기술과 WPKI 기술에 있어 우리 나라는 세계적으로 기술을 앞서나가며 주도하는 입장이라고 볼 수 있다. 그러나 이들을 뒷받침하는 관련 알고리즘이나 프로토콜, 스마트카드 기술은 아직 세계적으로 몇걸음 뒤쳐져 있는 것이 사실이며, 이러한 상황이 계속된다면 세계적으로 기술 표준 제정의 주도권을 항상 외국에게 빼앗기는 결과를 낳게 된다.

WPKI를 비롯한 여러 기술들이 아직까지 표준이 명확하게 구성되지 않았으며, 이에 따라 국내 업체들도 단지 외국 업체나 단체가 만들어 놓은 규격이나 표준을 이용한 제품 구현에 머물지 않고 표준 제정에 기여를 하여 세계 시장에서 주도권을 쥘 수 있어야 하겠다.

앞으로는 인증, 로밍, 지불 서비스, 금융 서비스 등의 다양한 기능을 가진 스마트카드가 원칩으로 구현되고, 이를 이용하여 무선 뱅킹, 무선 전자지불서비스, 무선 증권 서비스 등과 같은 무선 전자상거래 관련 응용들이 다양한 형태로 나타나게 될 것이다. 중요한 것은 이들 응용이 요구하는 보안 서비스를 정확히 분석하고, 기반 기술을 이용하여 어떻게 이들을 달성할 수 있는지를 찾아내는 것이다. 각 기반 기술과 프로토콜의 성격과 장단점을 정확히 분석하여 새로운 제품 혹은 응용이 요구하는 보안성과 편의성을 동시에 만족시킬 수 있도록 노력을 기울여야 한다.

참 고 문 헌

[1] WAP, "Wireless Application Protocol Architecture Specification", WAP Forum, http://www.wapforum.org/, 2001. 7.

[2] WMLScript, "Wireless Markup Language Script", WAP Forum, http://www. wapforum.

org/, 2000. 10.
[3] WTLS, "Wireless Transport Layer Security Protocol Specification", WAP Forum, http://www.wapforum.org/, 2000. 4.
[4] WMLScript Crypto, "WMLScript Crypto API Library", WAP Forum, http://www.wapforum.org/, 2001. 6.
[5] WTP, "Wireless Transaction Protocol Specification", WAP Forum, http://www.wapforum.org/, 2001. 7.
[6] WDP, "Wireless Datagram Protocol Specification", WAP Forum, http://www.wapforum.org/, 2001. 6.
[7] WIM, "Wireless Identity Module Specification", WAP Forum, http://www.wapforum.org/, 2001. 6.
[8] Vodafone, Telstar, Certicom, "Change Request WMLScript Crypto API", WAP Forum, http://www.wapforum.org/, 2001. 6.
[9] VeriSign, "Change Request WMLScript Crypto Library Specification", WAP Forum, http://www.wapforum.org/, 2001. 8.
[10] WPKI, "Wireless Application Protocol Public Key Infrastructure Definition", WAP Forum, http://www.wapforum.org/, 2001. 4.
[11] WAPCert, "WAP Certificate and CRL Profiles Specification", http://www.wapforum.org/, 2001. 5.
[12] Microsoft, "Mobile Phones", http://www.microsoft.com/mobile/phones/default.asp
[13] LEAP, "Overview of the LEAP Protocols", LEAP Forum, http://www.leapforum.org/, 2000. 8.
[14] NTT, "What is i-mode", http://www.nttdocomo.com
[15] Tomihisa Kamada, "Compact HTML for Small Information Appliances", http://www.w3.org/TR/1998/NOTE-compactHTML-19980209/, 1998. 2.
[16] Microsoft, "Microsoft Mobile Explorer 1.0 Specification", 1999. 5.
[17] T. Dierks, C. Allen, "The TLS Protocol", IETF RFC 2246, http://www.ietf.org/rfc/rfc2246.txt, 1999. 1.
[18] T. Dierks, E. Rescorla, "The TLS Protocol Version 1.0", IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc2246-bis-01.txt, 2002. 3.
[19] S. Black-Wilson, D. Hopwood, J. Mikkelsen, T. Wright, "Transport Layer Security (TLS) Extensions", IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-tls-extensions-04.txt, 2002. 5.
[20] Alan O. Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol version 3.0, Internet Draft", http://home.netscape.com/eng/ssl3/, 1996
[21] Third Generation Partnership Project, http://www.3gpp.org/
[22] 3GPP TS 33.102: "3G Security: Security Archi-tecture", V3.10.0, Dec. 2001.
[23] DaeHun Nyang, "Armoring password based protocol using zero-knowledge with secret coin tossing", 2001 IEEE International Symposium on Information Theory, pp 139-139, IEEE.
[24] T. Wu, "The Secure Remote Password Protocol", Internet Society Symposium on Network and Distributed Systems Security, pp. 97-111.
[25] D. Taylor, "Using SRP for TLS Authentication", IETF Internet Draft, 2001.
[26] D. Jablon, "Strong password-only authenticated key exchange", ACM Comp. Comm. Review, Vol. 26, No. 5, pp. 5-26.
[27] "무선 전자서명 인증서 프로파일 표준, ISTF-012", http://www.kisa.or.kr/standard/hwp/ISTF012.hwp, 2002. 4.
[28] "무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준", ISTF-013, http://www.kisa.or.kr/standard/hwp/ISTF013.hwp, 2002. 4
[29] "무선 WTLS 인증서 프로파일 표준", ISTF-013,

http://www.kisa.or.kr/standard/hwp/ISTF014.hwp, 2002. 4.
[30] "무선 전자서명 알고리즘 표준", ISTF-015, http://www.kisa.or.kr/standard/hwp/ISTF015.hwp, 2002. 4
[31] "무선 키분배 알고리즘 표준", ISTF-016, http://www.kisa.or.kr/standard/hwp/ISTF016.hwp, 2002. 4.
[32] "무선 인증서 요청형식 표준", ISTF-017, http://www.kisa.or.kr/standard/hwp/ISTF017.hwp, 2002. 4.

〈著者紹介〉

이 석 준 (Lee, Sokjoon)
1998년 2월 : 서울대학교 컴퓨터공학과 졸업
2000년 2월 : 서울대학교 컴퓨터공학과 석사
2000년~현재 : 한국전자통신연구원 무선인터넷보안연구팀 연구원
관심분야 : 암호학, 전자상거래, 무선LAN 보안

정 병 호 (Chung, Byung-Ho)
1988년 2월 : 전남대학교 컴퓨터과학과 졸업
1988년~2000년 : 국방과학연구소 선임연구원
2000년~현재 : 충남대학교 컴퓨터과학과 박사과정, 한국전자통신연구원 무선인터넷보안연구팀장/선임연구원
1988년 2월 : 전남대학교 컴퓨터과학과 졸업
1988년~2000년 : 국방과학연구소 선임연구원
2000년~현재 : 충남대학교 컴퓨터과학과 박사과정, 한국전자통신연구원 무선인터넷보안연구팀장/선임연구원
관심분야 : 무선인터넷 보안, 이동통신, 무선LAN 보안

정 교 일 (Chung, Kyoil)
정회원
1981년 2월 : 한양대학교 전자공학과 졸업
1983년 8월 : 한양대학교 전자계산학과 석사
1997년 8월 : 한양대학교 전자공학과 박사
1980년 12월~1981년 11월 : 엠시스템즈 사원
1982년 3월~현재 : 한국전자통신연구원 정보보호기반연구부장/책임연구원
관심분야 : IC카드, Security, Biometrics, 국가기반보호, 신호처리