무선 암호화 통신을 위한 연구

채철주, 최병선, 이재광
한남대학교

Research of secure cryptographic wireless communication

Cheol-Joo Chae, Byung-Sun Choi, Jae-Kwang Lee
Dept of Computer Engineering, Hannam University

요 약

현재 무선 인터넷 시장이 급속도로 발전하고 있고 여러 가지 콘텐츠 및 전자 거래 서비스가 유선상에서 제공하는 것처럼 서비스를 제공하고 있다. 국내에서는 휴대폰을 중심으로 각종 서비스들이 제공되고 있는 실정이다. 그러나 휴대폰은 유선상의 PC와 성능을 비교하면 절대적인 열세에 있다. 다시 말해서, 유선의 서비스처럼 안전한 보안을 바탕으로 제공하는 서비스가 아니라 하드웨어 성능의 열세로 인한 안전하지 못한 서비스이다. 이를 보완하기 위해 단말기 사양에 맞는 표준안들이 국제 포럼에서 계속해서 제정 중에 있으며 효과적인 보안통신을 위한 여러 연구들이 진행 중에 있다. 무선용 인증서를 사용하여 안전한 암호화 통신을 위한 연구로 무선 공개키 기반구조(WPKI :Wireless Public Key Infrastructure)가 있다. 본고에서는 이에 대해서 살펴보고 또, 무선용 프로토콜인 WAP포럼의 WAP(Wireless Application Protocol), Microsoft사의 ME(Mobile Explore) 그리고 일본 도코모사의 i-mode 중에서 가장 국제적으로 통용되어 쓰이고 있는 WAP에 대해서 살펴본다. 또한 현재 암호화 통신에서 사용되는 암호학적 안전성에 대해 논하고 안전한 무선 암호화 통신을 가로막는 요인과 해결 방안에 대해 논의한다.

1. 서론[1)]

현재 유선 상에 보안 서비스 즉, 인증, 무결성, 기밀성, 부인봉쇄, 접근 통제 서비스를 제공해주는 보안 기술로는 공개키 기반구조(PKI: Public Key Infrastructure)가 가장 일반적이라고 할 수 있다. 유선 인터넷 환경에서 보안 서비스는 PKI를 기반으로 안정적인 지원이 가능하다. 그러나 지금 활성화되고 있는 무선 인터넷 환경에서는 유선과 같은 보안 서비스를 제공하기 위한 환경이 제공되지 않고 있다. 유선 환경과는 다르게, 무선 환경에서는 무선 통신용 단말기가 갖는 제약사항 때문에 유선과 같은 보안 서비스를 제공하지 못하고 있는 실정이다. 이를 극복하기 위해서, 유선의 인증서와 다르게 인증서 경량화를 위한 규격, 무선 인증서 보관 및 갱신, 삭제에 대한 정의 그리고 인증서 검증 등에 관한 절차를 정의하고 있다. 그 밖에도 단말기의 처리 능력과 저장 공간을 해결해 주기 위하여 보안 모듈을 추가하고 있으며 이 보안 모듈은 인증서 저장 기능을 제공한다. 따라서 사용자의 비밀 정보와 인증서 저장, 전자서명 생성 및 검증, 암복호화 연산까지 보안 모듈로 어느 정도 유선과 같은 성능을 발휘할 수 있다. 따라서 본 논문에서는 2장에서 무선 PKI에 대한 개요 및 구조를 살펴볼 것이고, 3장에서 무선 PKI기술기준과 특징에 대해서 간략히 언급한다. 4장에서는 응용계층 보안과 무선 암호화 통신을 가로막는 요인을 설명하고 5장에서 결론을 내린다.

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

2. 무선 PKI

무선 환경에서 단말기의 제약 사항으로 인한 고려사항을 언급하자면 다음과 같다.

첫째, 단말기의 메모리 제약을 고려하여 인증기간과 상호연동 할 수 있는 인증서 요청, 관리 프로토콜을 적용하는 것이고, 둘째, 인증서 발급, 처리, 저장, 검증 등에 필요한 프로토콜을 무선에 적합하도록 모듈 크기를 줄이고 처리 시간 감소화하는 것이다. 세 번째는 무선인터넷 환경에 적합한 인증서 검증방식을 채택하여 단말기 컴퓨팅 능력으로 검증할 수 있도록 하는 것이다. 네 번째는 인증서, CRL(Certificate Revocation List) 프로파일 규격을 정하여 무선에 최적화하는 것이고 마지막으로 무선 단말기 상에서 실행할 수 있도록 서명, 검증, 암호화 알고리즘을 변경하여 최적화 하는 것이다.

휴대폰과 같은 이동 통신 장비가 보급화되면서 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 방식과 보안 모듈로써 자바 카드를 사용하고 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(Mobile Explore)같은 경우는 유선의 HTTP, TCP 프로토콜을 그대로 사용하는 경우이고, WAP의 경우는 무선 환경에 적합하도록 만든 프로토콜로써 유선과의 연동을 위해서는 WAP Gateway를 두어 유무선간 프로토콜 변경을 하고 있다. 본 고에서는 WAP을 기반으로 하는 무선 PKI를 논할 것이다.

무선 PKI의 구성요소에는 크게 인증서를 발급하고 인증서의 효력정지 및 폐지 기능을 하는 인증기관, 인증 기관과 사용자 사이에서 인증서 등록이나 신원을 확인하는 등록 기관, 인증서나 CRL을 저장하는 DB 그리고 사용자로 나눌 수 있다. 현재 WPKI 구조는 (그림1)과 같이 유선의 형태와 비슷하나, 이동통신 단말기의 제약사항으로 인해 자바카드 사용과, 인증서 검증을 위한 OCSP 사용으로 양측간에 인증을 통한 안전한 통신을 제공한다. 여기서 보여지는 End-to-End 보안의 개념은 WALS(Wireless Application Layer Security)(그림2) 전자서명 함수 및 암복호화 함수를 사용하여 제공하고 있다. 또 단말기에서

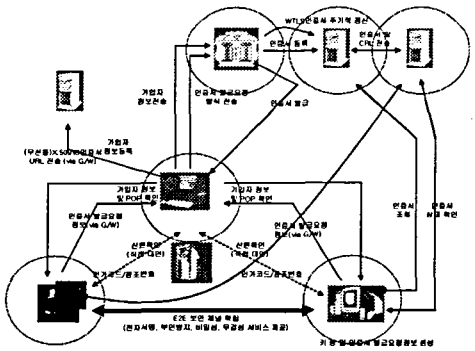

그림1 WPKI 구조[1]

안전한 통신을 위한 보안 모듈(WIM)을 사용하고 있다(그림2). 이는 WAP에서 전송계층 보안을 담당하는 WTLS에서 난수 생성 함수도 지원토록 하고 있다. 이 난수는 Hello 메시지 교환에 사용되고 양측의 실제 통신하는 암호 알고리즘 키 재료로도 사용된다. 이렇게 단말기에서 WIM을 이용하여 난수 생성 함수와 전자 서명에 사용될 함수를 제공하여 응용계층 암호화 통신을 가능하게 하고 있다. 이는 기존의 단말기의 제약사항을 해결하기 위한

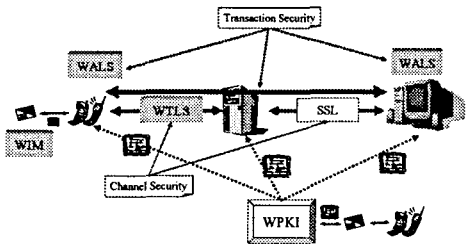

그림2 자바 카드를 사용하는 구조

직접적인 방법이다. 보안모듈을 사용하는 구조는 그림2에서 보듯이 전자 서명을 처리할 수 있고,

암복호화 함수를 제공하여 End-to-End 보안을 제공하고 있다. 다시 말해서 전송 계층의 WIM(Wireless Identity Module)과 응용 계층의 signText 함수와 Encrypt/Decrypt 함수를 사용하여 종단간 보안을 제공하고 있다. 이는 WAP 기반의 보안상 허점인 유무선 프로토콜 변환 시에 평문이 노출되는 위험요소를 해결하여 응용계층 보안 채널을 생성한다. 각 함수에 대해서는 4장에서 다시 살펴본다.

3. WPKI 기술기준

현재 단말기의 성능은 계속해서 발전되어 PDA폰이 등장하고 보급화 단계에 있다 그러므로 단말기 제약사항은 옛 이야기가 될 수 있으나, 현존하는 낮은 단말기들에 대한 해결 방안을 아직까지는 묵과할 수 없으므로 현재 제안되고 있는 기술들에 대해서 논의하고자 한다. 먼저 전자서명 기술기준을 살펴보면 인증서에서 변화가 있는데, 유선에서 사용하는 인증서를 그대로 사용할 수 없으므로, 인증서 크기를 줄이고 새롭게 추가되는 필드로 Domain Information이 있다. 이는 WAP에서 Gateway에 보안 허점을 보완하기 위해서 제시된 서버와 게이트웨이를 묶는 secure domain을 말하고 있다. 이들의 정보를 알리기 위해서 인증서의 확장필드에 새롭게 추가되는 필드가 그것이다. 알고리즘 또한 키의 크기가 작은 것을 요구하고 있어 RSA보다는 크기가 작은 ECC 알고리즘을 권장하고 있고 인증서의 전송 방법으로는 유선상에서 전체 전송을 해도 무관하지만 단말기에서는 URL을 사용하여 CPU 부담을 줄이고 있다. 전자서명 생성키 또는 인증서를 DER 형태로 보안 모듈(WIM)에 저장하도록 정의하고 있으며, 키분배용 WTLS 인증서의 경우에도 일련번호와 확장영역을 제외시켜 인증서의 크기를 줄여 사용하는데, 인증서 검증을 위하여 유효기간이 최대 48시간 이내인 Short-lived 인증서를 발행하여 검증을 대신하고 있다. 이렇게 WPKI 기술기준에 대해서 알아보았듯이 단말기가 갖고 있는 제약사항을 극복하여 유선과 같은 보안 서비스를 제공하고 있다. 따라서 WPKI 특징을 다음과 같이 정리할 수 있다.

첫째, 무선 전자서명 인증서 프로파일에서는 단말기에서 인증서 처리부담을 감소시키고자 확장필드 중에 Authority Key Identifier 필드와 Subject Key Identifier 필드를 선택사항으로 정의하고 있다.

둘째, 인증서 검증과 관련하여 유선에서 제공하는 CRL 검증뿐만 아니라 OCSP(Online Certificate Status protocol) 서버를 통한 인증서 상태확인 기능을 제공하기 위하여 Domain Information 필드를 포함하여 단말기에서 OCSP 기능을 제공할 수 있도록 하고 있다.

셋째, 현재 유선에서 정의하고 있는 RSA 알고리즘을 단말기에 사용하기에는 키 생성시간 등의 문제점을 해결하기 전에는 힘든 상황이므로, 무선 전자서명 알고리즘으로는 ECDSA 알고리즘을 정의하였고, RSA 알고리즘도 추후 기술발전에 따라 적용가능할 것으로 판단되어 단말기에서 서명, 검증이 가능하도록 정의하고 있다.

넷째, 무선 WTLS인증서 프로파일은 콘텐츠 제공자(Content Provider)의 키 분배용 인증서로 사용하기 위하여 정의하고 단말기에서 CRL 검증의 부담을 줄이기 위해 Short-lived WTLS인증서를 사용할 수 있도록 하고 있다.

다섯째, 유선의 인증서 요청 및 관리 프로토콜(CMP)을 무선단말기에 전부 탑재하기에 부담이 따르므로 무선 단말기에서 온라인으로 인증서를 요청할 경우에 사용자 인증과 POP(Proof of Possession)을 동시에 해결할 수 있는 요청형식을 참조번호, 인가코드 기반의 해쉬함수를 통하여 구성하였고, 무선인증서 요청 형식 및 관리 프로토콜은 WAP Crypto Library에서 정의한 Signtext 함수를 적용하여 단말기에 구현시 메모리 사용량 및 코드 크기를 최소화할 수 있도록 구성하고 있다.[2]

4. 응용계층 메시지 암복호화

앞에서 설명했던 바와 같이 응용계층 암복호화 과정은 WTLS와 응용계층의 암호화 라이브러리인 WAP Crypto Library를 사용하며 제반 사항으로 WIM 모듈을 사용하여

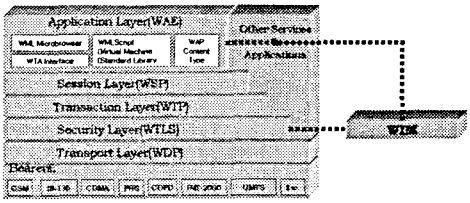

그림 3 End-to-End 보안 구조

제공한다. 여기서는 응용 계층에서 사용되는 함수들에 대
해서 언급하겠다. 먼저 전자 서명 함수에 대해서 살펴보면 다음 형식과 같다.

signedString =
Crypto.signText(*StringToSign, options, keyIdType, keyId*)

먼저 signText함수는 4개의 인수를 받아 서명된 값을 얻게되는데, 먼저 StringToSign은 전자서명될 데이터로 일반 텍스트 문자열(string)이다. 다음으로 options에는 서명 결과값인 signedString에 포함되는 선택적인 값으로 표1의 정수값을 갖는다.

표 1 옵션 필드[3]

	설 명
0x0 001	INCLUDE_CONTENT · 결과값에 전자서명할 데이터인 StringToSign을 포함한다.
0x0 002	INCLUDE_KEY_HASH · 결과값에 전자서명생성키에 대응되는 전자서명검증키의 해쉬값을 포함한다.
0x0 004	INCLUDE_CERTIFICATE · 결과 값에 전자서명 인증서 자체 또는 전자서명 인증서의 URL을 포함한다. · 만일 무선 단말기내에서 인증서를 획득할 수 없는 경우 결과값으로 "error:noCert"값을 반환해야 한다.

keyIdType는 전자서명검증키의 키식별자 유형을 나타내는 정수값으로 네 번째 파라미터인 keyId 내용이 결정된다. 각 값은 None(0), User_key_hash(1), Trusted_key_hash(2) 값이 될 수 있다. None값은 전자서명검증키 식별자를 사용하지 않는 경우에 쓰이며, User_key_hash값은 전자서명검증키의 해쉬값을 네 번째 파라미터에 넣을 때 사용한다. Trusted_key_hash값은 신뢰된 공인 인증기관의 전자서명검증키의 해쉬값이 사용될 때 사용되며 두 개 이상일 수 있다. 다음으로는 암호화 함수인데, 사용되는 파라미터인 flag는 다음에 오는 파라미

wapEnvelopedData = Crypto.encrypt(
flag,dataToEncrypt,recipientPublicKey, KeyManagementAlgorithm, contentEncryptionAlgorithm, rid_type, rid)

터를 어떻게 처리할 것인가를 나타내는 정보로써 각 문자가 하나의 옥텟으로 변환한 경우인지, 한글이 적용되었는지를 나타내고 있다. 두 번째 파라미터 dataToEncrypt는 암호화될 데이터이며, recipientPublicKey는 대칭키를 암호화하는데 쓰이는 수신자의 공개키 유형을 나타내는 정수 값이다. KeyManagementAlgorithm도 데이터를 암호하는 알고리즘을 나타내는 정수 값이다. contentEncryption- Algorithm은 dataToEncrypt를 암호화하는데 사용된 대칭키 알고리즘을 나타내는 정수값이다. rid_type은 수신자의 키식별자의 유형을 구분하기 위한 정수값이며, rid는 수신자의 키식별자 정보를 포함하는 데이터이다. 앞서 봤듯이 기본적인 함수의 파라미터 값은 인증서에 기반하고 있는 것을 알 수 있다. 이 파라미터 값은 OCSP에서 다운로드 하여 응용계층에서 암복호화 및 전자서명을 할 수 있는 것이다.

5 결 론

무선 인터넷 사용자가 해마다 폭발하듯이 늘어나고, 이러한 서비스 수요를 충족하기 위한 정보보호 시스템 개발이 진행 중에 있다. 무선 환경에서의 인터넷 서비스는 앞서 살펴보았듯이 유선과는 그 구조가 다르다. 단말기가 갖고 있는 제약사항 즉, 낮은 CPU 처리 능력, 제한된 메모리, 낮은 대역폭, 배터리 시간문제 등이 유선과 같은 정보보호 서비스를 가로막고 있다. 이에 본 논문에서는 무선 인터넷 환경의 제약사항을 극복하기 위한 방법으로 응용계층 보안에 대해서 알아보았다. 상대적으로 유선 암호화 통신에서 사용하는

키 크기를 사용하는 대신에 자바카드를 통하여 적은 메모리를 보완하고 암호화 연산을 도움으로써 안전한 통신을 위한 보안 서비스를 제공하고 있다.

6 참고자료

[1] 무선 인터넷을 위한 PKI 구축, 제6회 정보보호 심포지엄. 한국정보보호진흥원. 2001.7
[2] 무선 PKI 규격, TTA 저널 81호, p94~100
[3] ISTF_022 무선응용계층보안프로토콜 표준
[4] WAP-161-WMLScript Crypto-200010620-a
[5] WAP-260-WIM-20010712-a
[6] WAP-261-WTLS-20010406-a
[7] WAP-211-WAPCert-20010522-a
[8] WAP-217-WPKI-20010424-a
[9] WAP-219-TLS-20010411-a
[10] IETF RFC 2510(1993.3). Internet X.509 Public Key Infrastructure Certificate Management Protocols
[11] WAPFORUM, http://www.wapforum.org/