[5C-25]

무선 인터넷상에서의 WPKI에 대한 연구

이성현, 이원구, 이재광
한남대학교
shlee@netwk.hannam.ac.kr

Reserch of WPKI based on Mobile Internet

Seoung-Hyun Lee, Won-Coo Lee, Jae-Kwang Lee
Dept of Computer Engineering, Hannam University

요 약

먼저 본 논문에서는 WPKI(Wireless Public Key Infrastructure)에 대한 개요와 특징을 소개 및 분석하고, 유선의 PKI와는 다르게 무선의 형태에 적합한 WPKI 구조로 인증서 검증 방안과 단대단 보안을 제공하기 위한 방법에 대해 논의하였다. 인증서 검증 방안의 경우에는 OCSP(Online Certificate Status protocol) 서버를 통하여 인증서를 검증하고, 인증서 전체 수신 대신에 필요한 정보만을 다운로드하여 응용계층에서 전자서명 및 암복호화 함수를 사용함으로써 단대단 보안까지도 제공할 수 있다. WPKI에서 사용하는 기술기준으로 WIM(Wireless Identity Module)에 대해서도 언급해봤으며, 응용 계층에서의 메시지 암복호화, 전자서명 기술기준에 대해서도 살펴보고 결론을 내렸다.

1. 서론[1)]

인증, 무결성, 기밀성, 부인봉쇄, 접근 통제 등의 보안 서비스를 제공해주는 보안 기술로는 공개키 기반구조(PKI: Public Key Infrastructure)가 가장 일반적이라고 할 수 있다. 또한 유선 인터넷 환경에서 무선 인터넷 환경으로의 변화 추세에 따라 무선 환경에서도 유선과 같은 보안 서비스를 제공하기 위해서 공개키 기반구조를 요구하게 되었다. 그러나 유선 환경과는 다르게, 무선 환경에서는 무선 통신용 단말기가 갖는 제약사항 때문에 유선과 같은 보안 서비스를 제공하지 못하고 있다. 이를 극복하기 위해서, 인증서 규격에 대한 정의, 인증서 보관 및 갱신/삭제에 대한 정의 그리고 인증서 검증 등에 관한 절차가 요구된다. 그 밖에도 단말기의 처리 능력과 저장 공간을 해결해 주기 위하여 보안 모듈을 추가하는 방식이 표준으로 채택되었으며, 이 보안 모듈은 자체 연산 기능과 저장 기능을 제공 할 수 있다. 따라서 사용자의 비밀 정보와 인증서 저장, 전자서명 생성 및 검증, 암복호화 연산까지 보안 모듈로 해결할 수 있다. 따라서 본 논문에서는 2장에서 무선 PKI에 대한 개요 및 구조를 살펴볼 것이고, 3장에서 무선 PKI기술기준과 특징에 대해서 간략히 언급한다. 4장에서는 무선 단말기와 서버간의 인증 및 키 분배와 메시지의 암복호화 과정에 대해서 설명하고 5장에서 결론을 내린다.

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

2. 무선 PKI

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