학술정보 콘텐츠 제공을 위한 모바일 보안 서비스에 관한 연구

Mobile Security for Academic Information Service

김상국*, 최병선*, 강무영*
한국과학기술정보연구원*

Kim sang-kuk*, Choi byeong-seon*, Kang mu-yeong*
Korea Institute of Science and Technology Information*

요약

모바일 네트워크 환경은 언제 어디서나 네트워크를 사용하는 모바일 서비스를 편리하게 사용할 수 있도록 해준다. 그러나 모바일 단말기의 제약과 기존 무선 네트워크 환경의 보안 문제로 인하여 많은 보안 취약점을 가지고 있다. 이에 본 논문에서는 국내 모바일 표준 플랫폼인 WIPI에 세션키와 공개키를 조합함으로서 최소한의 암/복호화 연산을 수행하는 방식으로 PKI 서비스 구조를 제안하였다. 제안된 국내 표준 암호 알고리즘 기반의 안전한 인증 시스템은 모바일 네트워크 보안에 더욱 견고함을 더하여 줄 것이고, 향후 KISTI의 모바일 학술정보 콘텐츠 제공에 있어 안전한 서비스를 제공할 것이다.

Abstract

Mobile network environments are the environments where mobile devices are distributed invisible in our daily lives so that we can conventionally use mobile services at any time and any place. But, Mobile devices has a many security vulnerabilities caused by lower computing of devices and security problem of wireless network. So in this paper, PKI structure is proposed to minimize encrypting and decrypting operation by compounding session key and public key on WIPI environment. Proposed secure authentication system based on korean standard cryptography algorithm will give a more firmness in mobile network and support a more secure service for mobile academic information service that KISTI future plan.

I. 서 론

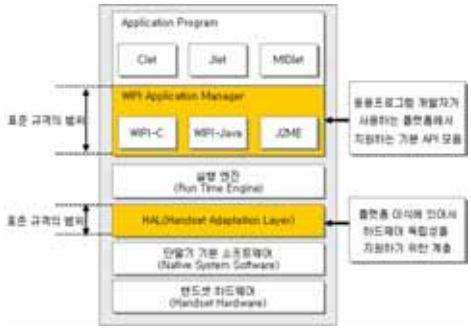
최근 컴퓨터가 주변 사물 및 환경 속으로 스며들고, 이들이 네트워크로 연결되어 인간의 삶을 편리하게 하는 유비쿼터스(ubiquitous) 환경이 급속히 도래하고 있다. 향후 유비쿼터스의 실현은 실세계의 각종 사물들과 물리적 환경 전반 즉, 물리공간에 걸쳐 컴퓨터들이 편재되게 하되 사용자에게는 겉모습이 드러나지 않도록 환경 내에 효과적으로 심어지고 통합되는 새로운 정보통신 환경의 구축이 예상된다[1][2]. 이에 본 연구에서는 기존의 데스크 탑이나 노트북에서 제공되었던 학술정보 서비스를 모바일 단말기에서 제공하기 위해, 기존의 AAA(Authentication, Authorization, Accounting) 서비스를 유비쿼터스 환경에서 가장 대표적인 휴대 장치인 모바일 단말기에 적용하여 보안 서비스를 제공할 수 있는 방법을 연구하였다. 본 연구에서의 모바일 보안서비스는 모바일 단말기에 인증서를 사용하여 세션키와 공개키의 조합으로 효율적인 인증 및 전자 서명 기능을 제공할 수 있는 PKI 기반의 인증 시스템으로서, 특히 모바일 단말기는 무선인터넷 표준플랫폼인 WIPI(Wireless Internet Platform for Interoperability) 환경을 고려하였다.

II. 관련 연구

2.1 WIPI

WIPI는 한국무선인터넷표준화포럼(Korea Wireless Internet Standardization Forum: KWISF)에서 만들어진 모바일 표준 플랫폼 규격으로 이동통신 단말기에 탑재되어 무선 인터넷을 통해 다운로드된 응용 프로그램 실행 환경을 제공하는 데 필요한 표준규격이다. 기존의 이동통신사들(STK, KTF, LGT)은 SKVM, GVM, BREW 등 각기 다른 무선 인터넷 플랫폼을 사용하여 왔다. 이와 같이 각각의 이질적인 플랫폼으로 인해 나타날 수 있는 응용 프로그램 실행 환경의 혼재와 로열티 문제로 발생될 수 있는 콘텐츠 업체들의 개발 부담과 상호 호환이 불가능한 상황에서 발생 가능한 중복투자 문제를 해결하기 위해 WIPI 개발이 진행되었다. WIPI는 국내 이동통신 3사, 전파연구소, TTA, ETRI 등이 2001년 하반기부터 여러 콘텐츠업체, 단말기제조사 및 기타 관련업체들의 의

견을 수렴하며 약 1년에 걸쳐 만들어낸 단말기 미들웨어 표준 플랫폼규격으로서, 2002년 5월 한국정보통신기술협회단체 표준인 TTAS-KO-06.0036(모바일 표준 플랫폼 규격)으로 채택되었다[3][4]. 다음 <그림 1>은 WIPI의 개념적 구조도를 보여주고 있다.



▶▶ 그림 1. WIPI 구조도

2.2 PKI

전자서명 기술을 효과적으로 이용하기 위해서는 공개키 암호 방식이 필요하며, 공개키 암호 방식을 이용한 인증 방법을 구현하기 위한 기술적, 제도적 기반이 요구되는데 이를 공개키 기반 구조(Public Key Infrastructure; PKI)라고 한다. 사용자는 PKI 클라이언트의 기능인 전자서명 및 검증, 기밀성 키 교환, 키 쌍 생성을 통해서 서버로부터 제공되는 접근제어, 기밀성, 무결성, 인증, 부인-봉쇄 등의 서비스를 제공받는다[5][6].

III. 안전한 모바일 인증시스템 설계 및 구현

3.1 PKI 시스템 설계

본 논문에서의 WIPI 기반의 PKI 시스템은 모바일 단말기를 사용하는 클라이언트가 모바일 콘텐츠 및 모바일 뱅킹 등과 같은 유료 서비스를 제공받고자 할 때, 안전한 인증 및 과금 체계가 적용될 수 있도록 인증 및 전자서명 서비스를 제공한다. PKI 시스템은 오프라인상의 사용자 인감이나 서명을 공개키 알고리즘을 이용해서 전자적으로 구현한 사용자 인증 시스템이다.

3.2 구성 및 기능

모바일 단말기를 위한 PKI 시스템은 <그림 2>와 같은 시스템 구성을 가지고 있다.

▶▶ 그림 2. PKI 시스템의 구성과 역할

3.3 인증 모듈

본 논문에서 제안하는 인증시스템은 자체 구축한 CA에서 발급받은 인증서를 WIPI가 탑재된 휴대단말기에 저장하고, 비밀키와 공개키 알고리즘을 사용하여 안전한 로그인 기능을 제공한다. 인증서에서의 공개키 알고리즘은 KCDSA와 RSA를 선택하여 발급받을 수 있으며, 인증이 완료됨과 동시에 세션키를 동기화한다. 다음 <표 1>은 인증과정을 설계하는데 사용한 표기들이다.

[표 1] 사용자 인증 프로토콜 표기

표기	의미
E, D	암호화(Encryption)와 복호화(Decryption)
CA	인증기관(Certificate Authority)
MC, MS	모바일 클라이언트와 모바일 서버
$CERT_{MC}$	모바일 클라이언트 인증서
$CERT_{MS}$	모바일 서버 인증서
SR_{MC}, SR_{M},	MC와 MS가 생성한 난수 값
PRI_{MC}, PUB_{MC}	모바일 클라이언트의 개인키와 공개키
PRI_{MS}, PUB_{MS}	모바일 서버의의 개인키와 공개키
secretkey	비밀키(Secret Key)
sessionkey	세션키(Session Key)
AutoInfo	인증이 성공했음을 포함하는 인증 메시지
SEED	국내 표준 대칭 암호 알고리즘(SEED)
RSA	비대칭 암호 알고리즘(RSA)
KCDSA	국내 표준 전자서명 알고리즘(KCDSA)
‖	연접(concatenate) 연산자

모바일 네트워크에서 안전하게 정보를 전송하기 위해서는 먼저 클라이언트와 서버 또는 기기간 상호인증 및 키 동기화(세션키) 과정이 필요하다(<그림 3> 참조).

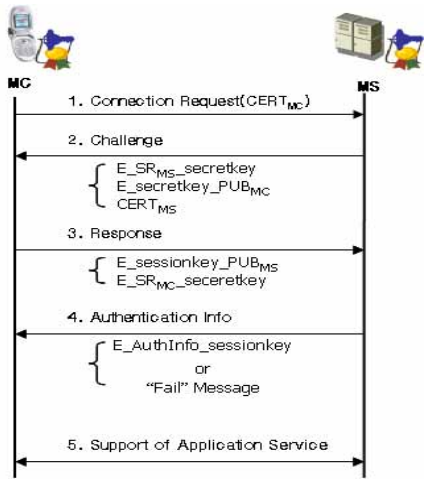


그림 3. MC와 MS의 인증절차

3.3.1 Connection Request

[MC -> MS] : 모바일 클라이언트(Mobile Client)가 모바일 서버(Mobile Server)로 접속을 요청한다. 이때 MC는 자신의 인증서($CERT_{MC}$)를 MS로 전송한다.

3.3.2 Challenge

- [MC <- MS] : MS가 E_SR_{MS}_secretkey와 E_secret_PUB_{MC}, $CERT_{MS}$를 MC로 전송한다.

① MC의 연결요청과 인증서를 수신한 MS는 CA에게 인증서의 유효성 검사를 요청한다.
② MC의 인증서가 유효한 경우, 서버는 SecureRandom 함수를 이용하여 난수(SR_{MS})를 생성하고, 이를 SEED 기반의 비밀키(secretkey)를 사용하여 암호화 한다($E\_SR_{MS}\_secretkey$).
③ secretkey를 안전하게 전송하기 위해, $CERT_{MC}$로부터 획득한 RSA 기반의 공개키(PUB_{MC})를 사용하여 암호화한다($E\_secretkey\_PUB_{MC}$).
④ MS는 자신의 인증서를 전송한다($CERT_{Ms}$).

3.3.3 Response

- [MC -> MS] : MC가 E_sessionkey_PUB_{MS}와 E_SR_{MC}_secretkey를 MS로 전송한다.

① MS로부터 인증서를 수신한 MC는 CA에게 인증서의 유효성 검사를 요청한다.
② MS의 인증서가 유효한 경우, MC는 자신의 개인키(PRI_{MC})를 사용하여 MS로부터 수신한 secretkey를 복호화한다($D\_secretkey\_PRI_{MC}$).
③ 복호화한 secretkey를 사용하여 SR_{MS}를 복호화한다($D\_SR_{MS}\_secretkey$).
④ MC는 자신의 난수(SR_{MC})를 생성하고, 이를 secretkey로 암호화한다($E\_SR_{MC}\_secretkey$).
⑤ MC는 자신이 생성한 SR_{MC}와 복호화한 SR_{MS}를 연접($SR_{MS} \| SR_{MC}$)하여 16바이트(SEED는 128비트의 키를 사용)의 세션키(sessionkey)를 생성하고 이를 $CERT_{MS}$로부터 획득한 공개키(PUB_{MS})를 사용하여 암호화한다($E\_sessionkey\_PUB_{MS}$).

3.3.4 Authentication Info

- [MC <- MS] : MS가 인증 여부를 MC로 전송한다.

① secretkey를 사용하여 SR_{MC}를 복호화한다.
($D\_SR_{MC}\_secretkey$).
② 복호화한 SR_{MC}와 MS 자신의 SR_{MS}를 연접하여, 16바이트 sessionkey를 생성한다($SR_{MS} \| SR_{MC}$).
③ MS의 개인키(PRI_{MS})를 사용하여 MC로부터 수신한 sessionkey를 복호화한다($D\_sessionkey\_PRI_{MS}$).
④ MS는 바로 이전의 ②에서 생성한 sessionkey와 ③에서 복호화한 sessionkey를 비교한다. 만약, 두 키가 일치한다면 sessionkey를 동기화하고 MC에게 인증이 성공했음을 알리는 메시지를 동기화한 sessionkey를 사용하여 암호화한다($E\_AuthInfo\_sessionkey$). 그러나 두 키가 일치하지 않는다면, 인증이 실패했음을 알리는 메시지를 생성한다(Fail).

3.3.5 Support of Application Service

- [MC <-> MS] : 인증이 성공한 경우 MS에게 응용 서비스를 제공받을 수 있다.

① MS로부터 "Fail" 메시지를 수신한 경우, Connection Request부터 재시도 한다.
② sessionkey로 AuthInfo를 복호화하여 인증이 성공했음을 알게 된다($D\_AuthInfo\_sessionkey$).
③ 동기화한 sessionkey를 사용하여 안전하게 데이터를 송수신 하며, MS는 MC에게 요청 서비스를 제공한다.

3.4 인증 모듈 및 전자서명 모듈 테스팅

인증서를 활용한 보안 모듈은 에뮬레이터와 서버에 보안 모듈 및 API가 탑재된 상태에서 실행되었다. 다음 <그림 4>는 SKT의 WIPI 2.0 에뮬레이터를 통하여 보안서비스를 구동시킨 화면이다.

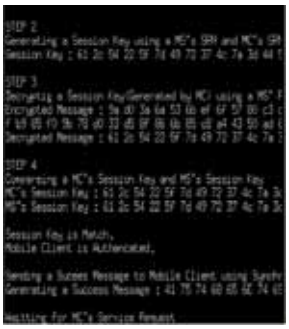
▶▶ 그림 4. WIPI 에뮬레이터 수행 화면

다음 <그림 5>는 모바일 클라이언트(MC)가 모바일 서버(MS)에 접속하여 인증을 수행하는 화면이고, <그림 6>은 모바일 데이터에 암호화 및 전자서명을 수행하는 화면이다.

▶▶ 그림 5. 모바일 인증(MC)

▶▶ 그림 6. 전자서명 생성(MC)

이전에 설명하였던 인증과정이 성공하면, MC와 MS는 동기화된 세션키를 통하여, MS가 MC에게 안전한 서비스 제공을 수행하게 되며, 전자서명은 안전한 데이터전송 및 신원확인기능을 제공하게 된다. 다음 <그림 7>은 위의 <그림 5>와 통신하는 MS가 MC의 인증 정보를 입력받아 처리하는 화면이다. MS는 MC와의 인증과정을 통하여 세션키를 동기화한다.



▶▶ 그림 7. 모바일 인증(MS)

▶▶ 그림 8. 전자서명 검증(MS)

그리고 <그림 8>은 이전의 <그림 6>과 통신하는 MS가 MC로부터 암호화된 데이터와 전자서명 값을 전달받아 데이터를 복호화하고, 이에 대한 전자서명 검증을 통하여 MC의 데이터와 신원을 확인한다.

IV. 결론 및 향후연구

모바일 네트워크 환경은 언제 어디서나 네트워크를 사용하는 모바일 서비스를 편리하게 사용할 수 있도록 해준다. 그러나 모바일 단말기가 가지는 제약 때문에 보안에 큰 취약점을 가지고 있다. 이에 향후 안전한 모바일 학술정보서비스 제공을 위하여 모바일 환경에 PKI 시스템을 적용하였으며, 본 연구를 통해서 구현된 PKI 시스템은 학술 정보 서비스를 위한 모바일 단말기 사용자뿐만 아니라, 각 기관이 가지는 사용자, 주 활용 형태, 기관 특성 등에 맞게 구축할 수 있는 중·소규모의 인증 체계를 수립하는 것을 목표로 연구하였다. 또한 모바일 단말기가 가지는 하드웨어적 제약 사항을 극복하고자, 모바일 단말기에 적합한 인증서 관리 서비스와 자바 기반의 암호화 알고리즘을 설계 및 구현하였다. 또한 비밀키와 공개키를 조합하여 보다 안전한 인증을 제공할 수 있도록 하였으며, 세션키와 공개키의 조합을 통하여 안전한 전자서명을 제공할 수 있었다. 또한 국내 표준 암호 알고리즘인 SEED와 KCDSA를 모바일 단말기에 적용하여 테스트하여 보았다. 향후, 개발된 보안 API가 보다 빠른 성능을 발휘할 수 있도록 최적화 하고 빠른 수행 속도를 제공하는 타원 곡선(Elliptic Curve) 알고리즘을 적용한 EC-KCDSA와 ECDSA를 적용하면 모바일 단말기가 보다 빠르고, 보다 강력한 암호학적 강도를 제공하게 될 것이다.

▌참 고 문 헌▐

[1] 김건우, 정교일, "모바일 보안 프로젝트 연구 동향, 한국정보통신표준협회, 2005. 11
[2] 이상윤, 김선자, 김홍남, "한국 무선 인터넷 표준 플랫폼(WIPI)의 표준화 현황 및 발전 전망," 정보과학회지, 제22권 제1호, 2004. 1, pp.16-23.
[3] "TTA.KO-06.0036 모바일 표준화 규격," 정보통신단체표준, 2004. 6.
[4] 배석희, "모바일 플랫폼 표준화 동향 및 향후 발전 전망," TTA 저널, 제82호, 2002, pp.59-66.
[5] IETF, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.
[6] "인증업무준칙 v1.1", KISA, 2001. 11