무선 환경의 의료 인증 시스템

오근탁° 이윤배 이성태
조선대학교 전자계산학과
{gtoh°, yblee,}@chosun.ac.kr {stlee}@iscu.ac.kr

Remote Medical Authentication System on the Mobile Environment

GuanTack Oh° YunBae Lee SungTae Lee
Dept. of Computer Engineering, Chosun University, Gwangju, Korea

요 약

일반 사용자가 현재 접할 수 있는 무선인터넷은 SMS를 활용한 문자 형식의 정보제공이 대부분이고 유선의 인터넷과 같이 멀티미디어 서비스 그리고 실시간 전송속도, 사용자 환경, 거기에 보안 서비스까지 유선의 인터넷 서비스와는 비교가 되지 않게 그 이용환경이 열악한 상황이다.

오늘날 원격 환경의 진료시스템이 개발되고 있는데, 이들 시스템은 미래의 원격진료 즉, 병원에 직접가지 않고 집에서 바로 혈압, 심박수 등을 검사 받을 수 있는 시스템 개발의 기본이 되고 있다.

그리고 정보통신의 발전으로 모바일 PC 즉, 개인 휴대용 단말기(PDA:Personal Digital Assistants)가 의료 분야에서 PC를 대체하여 이동성, 편리성을 제공하는 전자 차트를 선보이고 있다. 그러나 PDA는 작은 몸체로 이동성 및 편리성 등이 PC보다 뛰어나지만, 해상도가 큰 이미지, 높은 처리 속도를 요구하는 작업 등을 처리하기에는 효율성이 낮은 문제점이 있다. 또한 정보를 공유 할 수 있는 데이터를 무선 환경으로 처리해야 하기 때문에 환자와 관련된 의료 영상 즉, MRI 사진이나 X-ray 사진 등을 의료 환경에 이용 하는 데는 보안 의 문제점을 가지고 있다 따라서 본 논문에서는 매우 빠르게 발전하고 있는 진단과 치료기술을 이러한 의료를 필요로 하는 사람들에게 제공하는 접근성의 보장 문제를 해결할 수 있는 대안으로 무선 환경의 의료 인증시스 템을 제안 하고자 한다.

1. 서 론

현재 네트워크 기술 발전으로 인하여 거의 모든 곳에 네트워크가 보급 되면서 학교, 병원 등의 건물 내에서도 네트워크에 연결하여 인터넷 접속 및 네트워크 작업 등을 할 수 있게 됐다. 또한, 인터넷을 통한 멀티미디어 기술이 발달되어 의료분야, 전자.전기 분야 등에 걸쳐 많은 기여를 하였다. 그래서 병원에서도 실시간으로 치료 및 진찰을 할 수 있는 원격진료시스템이 개발 되어 의사나 담당 간호사의 PC를 이용하여 환자의 정보, X-ray 촬영 사진 등을 담은 차트를 검색하고, 볼 수 있는 환경이 가능하게 되었다. 이런 원격의료시스템에 대한 연구는 현재 많은 곳에서 이루어지고 있지만, 실제 임상에서 사용되기 위해서는 이동성과 무선 환경의 데이터 교환으로 인한 보안의 문제가 발생하고 있다.

예를 들어, 지금 바로 수술에 들어가야 하는 환자가 있는데, 그 환자에 대한 기록과 CT촬영 같은 자료를 보기 위해서 다시 자신의 PC로 돌아가야 한다는 것이다.

물론 이동성을 위한 노트북과 같은 컴퓨터가 있지만, 아직 이동하기에는 무겁고, 일정한 공간을 차지하기는 마찬가지 이다.

그러므로 이 논문은 무선 네트워크기반으로 모바일 컴퓨터용 아키텍쳐인 WAP를 이용하여 휴대용 정보단말기인 PDA를 통해 임상에 필요한 데이터를 전송받아 실시간으로 환자에게 처방을 할 수 있는 시스템을 연구하였고 자료를 전송받는 도중에 발생할 수 있는 보안 문제를 인증시스템을 도입하여 의료분야에 기여할 수 있도록 제안 한다.

2. 관련연구

2.1 wap의 정보보호기술

이동통신을 이용한 응용 서비스로서 유선 인터넷에서의 전자상거래와 같이 무선 이동통신에서도 무선 단말기를 이용한 무선 전자상거래 서비스가 요구되고 이에 대한 보호 대책도 필수적으로 요구된다. WAP에서는 무선 인터넷 보안과 관련해서 WTLS, WPKI,WIM, WMLScript Crypto Library 등이 있다.
현재 기술하고, 아래에 각각에 대해서 간단히 소개한다.

2.2 WTLS(Wireless Transport Layer Security)

WTLS는 데이터그램 프로토콜인 WDP/UDP 위에서 동작하는데 서버와 클라이언트 간의 인증과 세션키를 생성, 분배하는 Handshake 프로토콜과 실제로 데이터에 대한 기밀성을 제공하는 Record 프로토콜로 구성
된다. 그 밖에 Alert 프로토콜과 ChangeCipher Spec 프로토콜로 이루어져 있다.
하지만, 무선 구간에서 WTLS로 암호화된 데이터는 게이트웨이에서 프로토콜 변환 과정을 거쳐 유선의SSL과 연동하는 과정에서 평문으로 복호되는 결함이있다.
그래서, 이 문제를 해결하기 위해 트랜스포트 계층에서 WTLS를 이용한 새로운 메커니즘이고려되어야 한다.

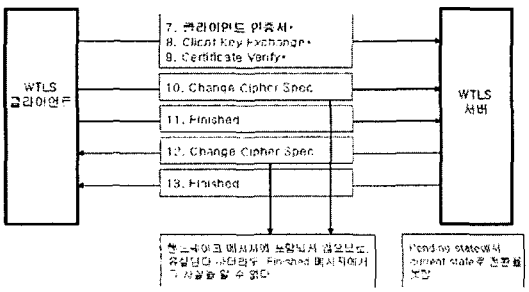
WMLScript Crypto Library

WMLScript Crypto Library는 WTLS에서 지원하지 않는 전자서명 기능을 응용 계층에서 Crypto.signText
함수를 이용해 부인봉쇄 서비스를 제공한다.

WIM(WAP Identity Module)

WTLS와 응용 레벨에서 보호 함수를 수행하는데 필요한 암호 연산을 지원하기 위해 비밀키 및 인증서를 저장한다. 무선 단말기의 취약한 보안을 위해 사용되는 요소로 스마트 카드로 구현된다.

2.3 WAP의 보안

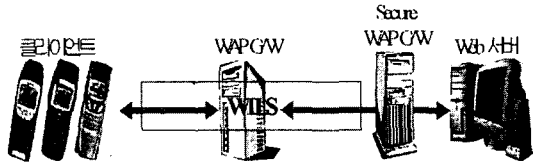


[그림1] WAP의 보안

무선구간 (WTLS (TLS) : 사용자로부터 전달된 데이터를 해독하고 다시 암호화 하여 웹 서버로 전달유선구간 (TLS (WTLS) : 웹 서버로 부터 전달된 데이터를 해독하고 이를 다시 암호화 하여 사용자에게 전달한다. 이 과정에서 WAP G/W는 사용자와 서버간 전달되는 데이터의 모든 내용을 해독. 보안의 허점이 노출되어 유선 인터넷과 같은 완벽한 END-TO-END 보안을 제공 하지 못한다. 따라서 본 논문에서는 원격진료 시스템의 이중 부분을 두 가지 방법에서 살펴보았다.

대안1: 응용수준에서 암호화를 수행하는 방법

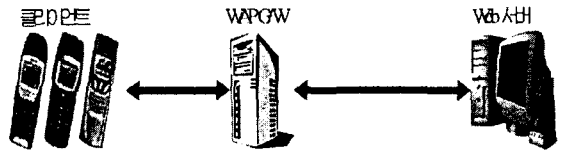
서버의 인증서를 가져와 세션키를 암호화 하여 암호문과 함께 전송하는 방식으로 WAP 규격에서 지원하지 않는 사설방식이다.



[그림 2] 방안

대안 2: Secure Domain

응용 서버가 신뢰하는 GATEWAY를 직접 운영하는 Secure Domain을 사용하면WAP 표준의 WTLS를 이용하여 신뢰할 수 있는 Client authentication 및 기밀성 보장이 가능하다.



[그림3] 방안 2

3. 구현

이 해결 방안으로 WPKI 를 제시한다.

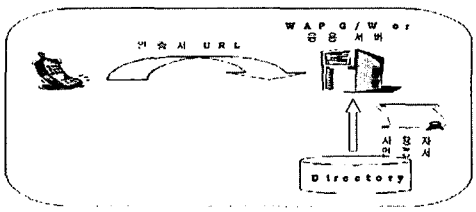
우선 유선의 PKI와 무선의 PKI간의 확실한 차이점은 인증서를 검증하는데 있다. 일반적으로 PKI시스템에서 클라이언트가 가지는 가장 큰 컴퓨팅 부하는 인증서를 클라이언트에 전달된 인증서를 검증하는 것이다.
전달된 인증서가 유효기간을 넘어선 것은 아닌지 그리고 클라이언트에서 검증할 수 있는 인증기관에서 배포된 것인지 또 해당 업무 등에 그 인증서를 사용할 수 있는 것인지에 대해서 먼저 알아보고 나서 서비스를 시작한다.
그러나 이러한 작업을 하기 위해서는 클라이언트에 인증서 폐지목록(Certificate Revocation List : CRL)을 포함한다 인증서를 검증할 정보들이 필요하다. 그러나 무선 인터넷 단말기는 우리가 일반적으로 사용하고 있는 PC의 환경과 아주 다르다. 즉 제한된 컴퓨팅 파워와 메모리를 가지고 있다. 그래서 이러한 문제를 해결하기 위해서 제안된 것이 Shot Lived Certificate, Online Certificate Status Protocol(OCSP) 방식의 인증서 검증 방법이다.
WPKI는 서버와 클라이언트 간의 인증을 위해 무선환경에 적합한 공개키 기반 구조를 제공한다. 유선 공개키 기반 구조와의 호환 등을 고려해서 일반적으로

서버는 WTLS에서 정의하는 인증서를 사용하고
클라이언트는 X.509v3 형식을 사용한다.
WPKI의 구성은 크게 사용자 등록을 담당하는 등록기관(RA), 인증서의 발급, CRL 발급 및 갱신 등을 담당하는 인증기관(CA), 인증서와 CRL 등을 보관하고 사용자가 access할 수 있는 디렉토리 서버(DS), 그리고 각각의 사용자의 단말기 환경에 적합하도록 최적화 된 Handset 모듈(무선용), PC client 모듈(유선용), CP 모듈(Contents Provider Server 용)로 구성되며, 필요에 따라서 인증기관에 종속되는 키 복구 시스템, OCSP 서버가 제공되어질 수 있다.

WPKI 인증서의 종류는 다음과 같다

WAP G/W 인증서

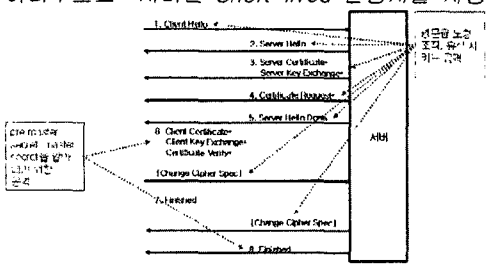
WTLS 서버인증용(minicert) 무선 사업자가 운영하는 WAP Gateway에 발급 무선으로 단말기에 전송한다.
사용자 및 서비수서버 인증서 WTLS 클라이언트 인증용(X.509 cert) 단말기에는 URL만 저장하고 WTLS 서버가 인 증시 디렉터리에서 가져온다.
전자서명용 (x.509 cert) 단말기에는 URL 만 저장하고 응용 서버가 서명 검증시 해당 디렉터리에서 가져온다.



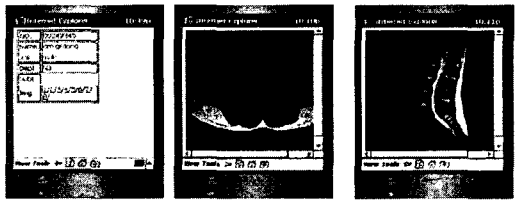
[그림 4] WPKI 인증서 구조 절차도

WPKI 구현 문제점 및 해결방안

CA 인증서 무결성 확인이 어려우므로 단말기에 데이터를 전송할 때CA 인증서를 전송 설치한다.
X.509 CRL 방식의 CRL목록을 이용한 인증서 검증이 어려우므로 서버는 Short-lived 인증서를 사용하였다



[그림 5] 보안 프로그램 개념도



1번 데이터전송 2번 이미지전송 3번 실행결과

[그림 6] 원격의료 인증 프로그램 결과화면

6. 결론 및 향후 연구 과제

즉 일반적인 기업이나 사용자들은 기존의 유선에서 사용하고 있던 응용 프로그램 즉 서비스를 보다 편리하게 보다 접근하기 쉽게 활용하기 위해서 무선 인터넷을 사용한다는 것이다. 그러자면 당연히 무선 인터넷 보안 또한 유선 인터넷의 보안 기술과 접목이 되어야 한다는 것이다
오늘날 원격의료가 새롭게 부각되는 것은 보통신기술의 발달이 원격의료를 뒷받침해 주고 있기 때문이기도 면서 새로운 의료서비스에 대한 제공자와 수요자들의 전환이 이루어지고 있기 때문이라고 할 수 있다. 매우 빠르게 발전하고 있는 진단과 치료기술을 이러한 의료를 필요로 하는 사람들에게 제공하는 접근성의 보장 문제를 해결할 수 있는 대안으로 원격의료가 떠오르고 있다. 원격의료의 도입 배경 역시 통신과 네트워킹 기술의 고도화를 기반으로 하여 원격영상기술, 원격자료전송 기술 등의 신기술이 개발되면서 본격화되기 시작하였다
원격의료가 환자, 의사 및 의료기관, 그리고 사회전체에 미치게 될 여러 가지 긍정적 효과들이 예상되면서 이에 대한 활발한 연구와 보안 관련 사업들의 추진이 전 세계적 으로 펼쳐지고 있다. 원격의료의 도입을 활성화의 원동력이 되고 있는 원격의료 인증 시스템 도입의 긍정적 효과는 사회적으로 미치는 효과는 대단하다 할수 있다.

6. 참고문헌

[1]Marchin Metter, "WAP enabling existing HTML applications", IEEE AUIC, Jan 31, 2000.
[2]Rick Bender, "Kentucky Field Inspection PDA Application" , IPEC, Conf2002, 2002.
[3] Jo & S 기획 저, "모바일 프로그래밍", 2002.
[4] 홍준호 외 2인 공저, "about WAP" 2001.
[5] 백철화, "원격진료의 발전 및 실례",
[6] http://www.cs.ncl.ac.kr/old/people/wyell.hanna/home.formal/.
[7] WAP White Paper, AU-System Radio. FEb.1999
[8] WAP White Paper, WAP Forum, June 1999.