공개키기반 u-Healthcare 전송 시스템의 구현 및 테스트

정선화, 백종혁, 박석천
경원대학교 소프트웨어학부
e-mail: scpark@kyungwon.ac.kr

Design and Implementation of Public Key-based u-Healthcare Transport System

Sun Hwa Jung, Jong Hyuk Baek, Seok Cheon Park
Division of Software, Kyungwon University

요 약

u-Healthcare는 의료 장비 및 센서 등을 이용하여 획득된 생체 신호 및 의료정보를 유·무선의 통신수단을 통해 지식 기반의 의료정보로 구축하고 이를 언제, 어디서, 누구든지 이용 가능한 실시간 u-Healthcare 지원 환경을 구축하여 지능형 의료정보 웹 포털 서비스를 제공하는데 목적을 두고 있는 서비스이다. 하지만 현시점에서의 시스템은 생체 신호 및 의료 정보 제공시에 보안에 대한 고려가 이루어지고 있지 않다. 이러한 자원들은 개인 프라이버시에 직결되는 것으로 보안의 필요성이 대두된다. 따라서 본 논문에서는 IP망에서 생체신호 전송을 위한 전송시스템을 설계하고 전송시 생체신호정보에 대해 사용자 인증과 암호화를 적용하여 u-Healthcare 전송시스템을 설계하고 구현하였다.

1. 서론

사회가 발전되고 고령화됨에 따라 건강과 복지에 대한 문제가 주요 관심사로 부상하고 있다. 이에 따라 우리나라에서도 근래에 정보통신기술을 이용하여 유비쿼터스 헬스케어(Ubiquitous Healthcare)에 대한 연구가 활발하게 진행되고 있다. u-Healthcare는 지금까지 의료기관을 중심으로 제공되었던 건강 진료 서비스를 가정과 개인에게까지 확대하는 것으로, 각 개인에 따라 차별화된 맞춤형 건강관리 서비스 제공을 지향 한다[1].

사용자의 생체신호를 측정하고 이를 유·무선 네트워크를 통해 병원으로 전송하여 피드백 받는 것은 u-Healthcare의 기본이 되는 서비스이다. 이를 위해서 생체신호 측정 단말기를 통하여 수집한 생체신호를 병원으로 전송하는 시스템이 필수적이다. 하지만 현재 개발되고 있는 시스템은 사용자의 생체신호정보 보안에 대한 문제점을 지니고 있다. 사용자의 생체신호정보는 개인의 프라이버시에 직결되는 것으로 보안의 필요성이 매우 큰 특성을 지닌다. 이와 같은 이유에서 IP망에서 생체신호 전송을 위한 시스템과 전송시 생체신호정보 보안에 대한 연구가 필요하다고 판단된다[2,3].

따라서 본 논문에서는 비밀보장, 무결성, 부인방지를 만족하기 위해서 공개키 암호화 알고리즘과 PKI (Public Key Infrastructure)를 통하여 사용자 인증과 암호화/복호화를 적용한 u-Healthcare 전송시스템을 설계하고 구현하였다.

2. 공개키 암호화 시스템

2.1 공개키 암호 알고리즘

공개키 암호 알고리즘은 연관되어 있는 두 개의 키를 이용하여 암호화하거나 복호화하는 알고리즘이다. 즉, 하나의 키로 암호화하고 나머지 다른 하나의 키로 이를 복호화할 수 있다. 따라서 키 쌍에서 하나의 키를 공개하고 다른 하나는 외부에 공개되지 않도록 보관한다[4].

공개키 방식은 두 가지 용도로 이용될 수 있는데,

하나는 송신자가 수신자의 공개키로 암호화하여 전송하였을 때, 수신자만이 복호화하여 정보를 얻을 수 있으므로 데이터 보호에 이용하는 경우와 송신자가 자신의 비밀키로 암호화한 데이터를 전송하였을 때 수신자가 송신자의 공개키로 수신한 데이터의 정보를 얻을 수 있으므로 송신자가 보낸 데이터라는 것을 확인할 수 있으며, 데이터를 보낸 사실에 대한 부인을 봉쇄할 수 있는 기능에 이용할 수 있다.

데이터를 암호화하고 통신하는 과정은 다음과 같이 이루어진다. 먼저 비밀키 알고리즘으로 데이터를 암호화한다[9]. 그리고 데이터를 수신할 사람의 공개키를 사용해 비밀키를 암호화하고, 데이터의 암호문과 비밀키의 암호문을 수신자에게 전송한다. 수신자는 자신의 개인키를 이용해 비밀키를 복호화하고 복호화한 비밀키로 암호문을 복호화해 실제 데이터를 얻는다[5][6]. 보통 암호화해야 할 전체 데이터의 양이 적더라도 공개키 암호 시스템을 사용해 데이터를 직접적으로 암호화하지 않고 위의 방식을 사용한다.

2.2 전자서명

공개키를 이용한 암호화 방식은 전자서명에도 이용될 수 있다. 공개키를 이용한 암호화에서는 공개키는 암호화에 사용되고 비밀키가 복호화에 사용되는 반면, 전자서명에서는 그 역으로 사용되어지게 된다.

즉, 송신자 A가 수신자 B에게 자신의 서명 문서를 전달하기 위해서는 A는 자신의 비밀키로 암호화를 한 후 B에게 전달하고, B는 A가 전달한 값을 받은 후 A의 공개키로 이를 확인하는 과정을 거친다. 이때 B가 받은 데이터는 A만이 생성할 수 있으므로 A가 보낸 것이 확실하다는 것을 검증할 수 있기 때문에 전달하고자 하는 정보에 대한 전자서명을 수행할 수 있게 된다. 이러한 과정으로 디지털 데이터로 작성된 문서에 작성자나 송신자의 도장을 찍는 것과 같은 효과를 얻을 수 있다[4].

그러나 네트워크상의 공개키가 신뢰가능한 사람의 공개키인가를 확인하는 문제가 존재한다. 이러한 문제를 해결하기 위하여 A와 B의 사이에 사용되는 공개키에 대한 무결성을 보장하기 위해 인증기관(Certification Authority)이 발행한 인증서(Certificate)의 사용이 필수적으로 요구된다.

2.3 인증 및 PKI

인증은 크게 두 가지 의미로 대변된다. 첫 번째는 전자 서명을 통하여 구현될 수 있는 사용자 인증 또는 메시지 인증을 의미하는 “Authentication”이고, 두 번째는 공개키 암호방식에서 공개키의 무결성을 보장하기 위해 인증기관이 발행하는 인증서의 의미를 갖는 “Certification”이다.

인증(Certification) 서비스의 필요성은 공개키 암호시스템의 사용에서부터 비롯되며, 안전한 전자상거래 환경 구축을 위해서는 인증, 무결성, 비밀성, 부인방지 등의 정보보호 서비스가 필수적으로 요구되며, 인증, 무결성, 부인방지 등의 서비스는 전자서명 기술을 활용함으로써 해결 가능하다.

공개키 암호기법을 이용한 전자 서명 기술은 수학적으로 그 안전성을 증명 할 수 있는 대표적인 인증(Authentication) 기법으로, 이것의 실제 적용을 위해서는 인증(Certification) 서비스가 필요하게 된다.

인증 서비스란 인증기관이 제공해 주는 인증서 발급, 인증서 관리 등 일련의 인증 관련 서비스를 통칭하는 것이다. 이를 위해서 공개키 암호방식을 이용한 전자서명 기술의 효과적인 이용이 요구되며, 공개키 암호방식을 이용한 인증 방법을 구현하기 위한 기술적, 제도적 기반이 요구되는데 이를 공개키 기반구조(PKI : Public Key Infrastructure)라고 한다[7,8][10]. PKI를 구축함으로서 암호키 갱신, 복구 위탁 등과 같은 키 관리, 인증서 생성 및 취소관리, 그리고 인증 정책관리와 같은 서비스의 제공이 가능해진다.

3. 공개키기반 u-Healthcare 전송시스템의 설계

본 모델은 인증 서버를 통하여 u-Healthcare 서버와 클라이언트 시스템(생체신호 전송시스템) 인증을 하고, 세션 정보 생성 및 데이터에 대하여 공개키 기반 TLS를 통하여 암호화함으로서 보안성을 강화하였다. 그림 1은 전체 시스템의 개요도를 나타낸 것이다.

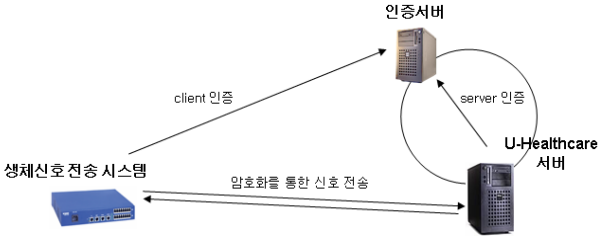

그림 1 전체 시스템 개요도

제안한 시스템의 메시지 동작 절차는 그림 2와 같으

며, 단계는 크게 PKI 인증단계, 생체신호전송시스템과 u-Healthcare서버와의 인증단계 그리고 암호화를 통한 안전한 생체신호 전송 단계로 분류할 수 있다.

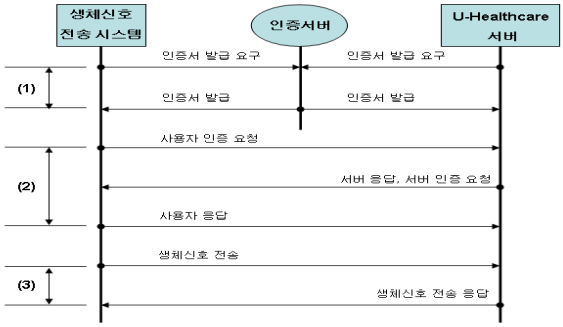

그림 2 제안 시스템의 동작 절차

그림 3은 제안한 시스템의 동작흐름도를 나타낸 그림이다.

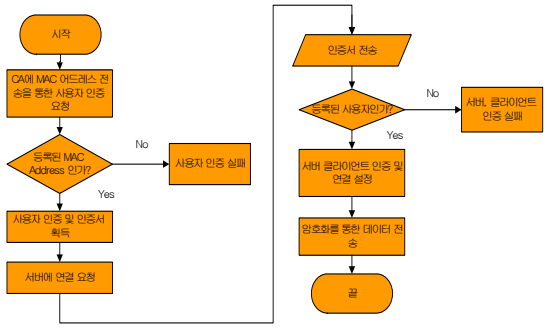

그림 3 제안 시스템의 동작흐름도

전송 계층 보안 프로토콜의 적용은 그림 4에서 나타낸 바와 같이 클라이언트와 서버간에 인증하는 절차로 이루어진다. TLS(Transport Layer Security)의 Full Handshake 과정은 클라이언트가 서버에게 Client Hello 메시지를 전송함으로써 시작한다.

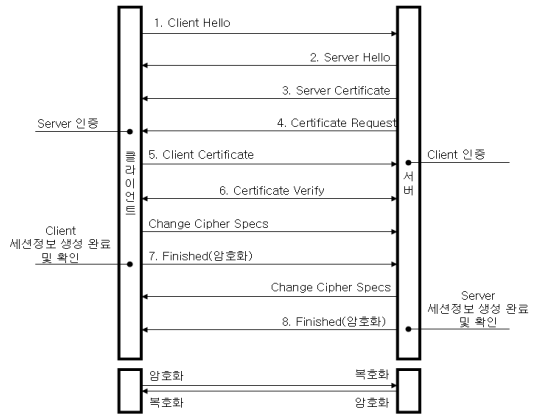

그림 4 전송계층에서의 데이터 전송 처리 절차

4. 공개키기반 u-Healthcare 전송시스템의 구현

4.1 구현 환경

공개키기반 사용자 인증과 암호화를 적용한 u-Healthcare 전송시스템은 Intel PXA 255-400을 탑재한 임베디드 보드를 기반으로 개발되었다. PXA 255가 지원하는 3개의 시리얼포트와 이더넷 통신환경이 구축되어 있으며, 하드웨어 디버깅을 할 수 있는 JTAG 포트도 내장되어 있다. 또한 임베디드 리눅스를 기반으로 많은 어플리케이션을 원활하게 이용하기 위한 64Mbyte의 램과 롬이 기본으로 탑재되어 있다. u-Healthcare 전송시스템의 구현 환경은 그림 5와 같이 구성하였다.

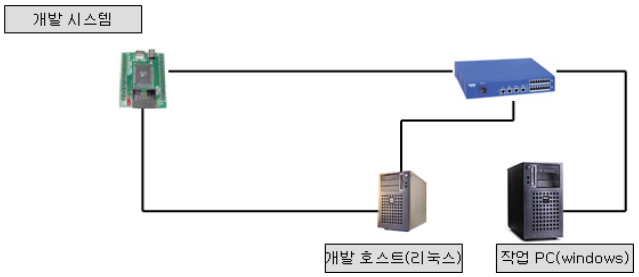

그림 5 전송 시스템의 구성

u-Healthcare 서버는 기반 운영체제로 RedHat Linux 9.0을 사용하였으며, 구현을 위한 언어는 c를 사용하였다. 구현을 위한 환경은 표 1과 같다.

<표 1> 구현 환경

구 분	구성요소		세부내역
하드웨어	u-Healthcare 전송시스템	PCB	100mm × 140mm
		MCU	400MHz PXA 255 ARM RISC Chip
		RAM	64 Mbytes SDRAM
		ROM1	512 Kbytes Boot Flash
		ROM2	64Mbytes NAND Flash
		Ethernet	CS 8900 10-Mbps
		Serial	RS-232C 3port
		USB	USB Client
		JTAG	ON-Board JTAG Convertor
		Extension Connector	160 pins Board to board Connector
	인증서버, u-Healthcare 서버	CPU	Pentium IV 2.66GHz
		그래픽 카드	Geforce2 MX440(64)
		메모리	256
		사운드카드	SIS7012 PCI
		이더넷카드	RealTek RTL-8139
소프트웨어	운영체제		RedHat Linux 9.0

4.2 구현

전송 시스템이 생체신호 측정단말기로부터 생체신호를 전달받아 인터넷망으로 전송하기 위한 시스템의 모듈 구조는 그림 6과 같다. 구현된 시스템은 RS-232C 시리얼 포트로 생체신호를 입력 받아 암

호화 모듈을 통해 암호화를 수행한 후 TCP/IP를 통해 u-Healthcare 서버로 패킷을 전송한다. 시스템내의 인증 모듈을 통해 시스템 인증을 수행하여 정당한 사용자만이 데이터를 전송할 수 있다.

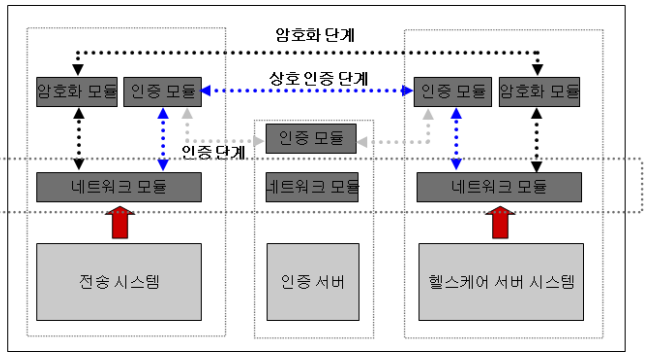

그림 6 u-Healthcare 전송시스템의 모듈 구조

클라이언트는 자신의 MAC 어드레스를 통하여 인증 서버에게 u-Healthcare 서버의 공개키를 요청하게 된다. 인증 서버는 클라이언트의 MAC 어드레스로 클라이언트를 인증하고 u-Healthcare 서버의 공개키를 인증서에 첨부하여 전송한다.

인증서를 통하여 클라이언트는 RSA 알고리즘을 사용한 512 bit의 u-Healthcare 서버의 공개키를 획득할 수 있다. 이 서버의 공개키를 이용하여 클라이언트와 서버간의 상호 인증을 수행한다.

u-Healthcare 서버는 먼저 서버의 공개키로 암호화된 클라이언트의 인증요청 메시지를 받아 자신의 개인키로 이를 복호화한다. 복호화가 가능하면 클라이언트 인증이 성공한 것이다. 클라이언트 인증이 성공하면 비밀키(DES Key)를 생성하여 이를 자신의 개인키로 암호화하여 클라이언트로 전송한다. 클라이언트는 이를 통하여 인증이 이루어진 것을 확인하고 비밀키를 통하여 생체신호를 암호화하고 이를 u-Healthcare 서버로 전송한다. u-Healthcare 서버는 이를 복호화하여 생체신호 데이터를 획득한다.

5. 결론

현재 개발되고 있는 u-Healthcare 시스템은 앞에서 언급한 바와 같이 하드웨어 및 서비스 중심의 구현에만 초점이 맞추어져 있기 때문에 이러한 보안에 대한 고려가 없는 상황이다. 이와 같은 이유에서 생체신호 전송에 있어서 보안에 대한 연구 수행이 필요하다고 판단된다.

따라서 본 논문에서는 공개키 기반의 사용자 인증과 암호화를 적용하여 인증, 기밀성 및 무결성을 구현한 u-Healthcare 전송 시스템을 제안하였다. 이를 위하여 생체신호를 분석하고 임베디드 시스템에 대하여 연구·분석하였다. 또한 비밀키 암호 알고리즘 및 공개키 암호 알고리즘과 PKI에 대하여 연구·분석하고 그 내용을 토대로 생체신호 전송시스템의 기본 기능인 서버와 통신하기 위한 네트워크 모듈과 전송시스템과 서버간의 인증을 위한 인증 모듈, 그리고 전송시스템과 서버간의 암호화 및 복호화를 위한 암호화 동작 절차를 설계하였다. 설계를 기반으로 클라이언트와 서버의 인증을 위한 인증 모듈과 클라이언트와 서버간에 암호화 및 복호화를 위한 암호화 모듈을 구현하였다.

향후 연구방향으로는 구현한 모듈을 바탕으로 테스트하기 위한 테스트베드를 구축한다. 구축된 테스트베드에서 인증 및 암호화를 적용한 경우와 그렇지 않은 경우의 전송 소요 시간을 측정하여 비교 성능 평가를 수행할 예정이다. 또한 패킷 데이터 스니핑을 통하여 전송 데이터의 공격 가능성을 검증할 예정이다.

참고문헌

[1] 손대일, “u-city에서 유비쿼터스 헬스케어의 방향”, 전자부품연구원 전자정보센터, 2005. 11.

[2] e-Health 시장동향 및 활성화 방안, etri, 2004. 11

[3] 박현규 외, “ZigBee를 이용한 생체신호 전송 및 관리시스템”, 한국컴퓨터종합학술대회, 2005.

[4] R. Rivest, A. Shamir and L. Adelman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems” Communications of the ACM, Vol.21, No.2, pp. 120-126, 1978.

[5] E. Rescorla, “Diffie Hellman Key Agreement Method”, IETF RFC 2631, 1999.

[6] T. Dierks, C.Allen, “The TLS Protocol Version 1.0”, IETF RFC 2246, 1999.

[7] 칼리슬 아담스외, “보안을 위한 효율적인 방법 PKI”, 인포북, 2003. 9

[8] Russ Housley, “Planning for PKI”, John Wiley & Sons, 2002.

[9] 한국정보통신 기술협회, “128비트 블록 암호 알고리즘 표준(SEED)”, 1999. 4.

[10] Mattbew Stallings, “Cryptography and Network Security Principles and Practice”, Green P.377-400, 2001. 2.