WBAN을 기반으로 한 OpenEMed의 PIDS를 이용한 Kerberos 인증

이재광*, 김영혁*, 임일권*, 이재필*, 이재광*
*한남대학교 컴퓨터공학과
e-mail : leejk@netwk.hannam.ac.kr

A study on WBAN based Kerberos Authentication System using PIDS of OpenEMed

Jae-Gwang Lee*, Young-Hyuk Kim*, Il-Kown Li,m*
Jae-Pill Lee*, Jae-Kwang Lee*
*Dept of Computer Engineering, Han-Nam University

요 약

인체 무선망이란 USN(Ubiquitous Sensor Network)을 통해 환자의 생체 정보를 실시간으로 수집하는 환경이다. 이를 기반으로 원격지에서 생체 정보를 전달 받는 시스템이 u-RPMS(USN Remote Patient Monitoring System)이다. u-RPMS에서 실시간으로 환자의 정보들이 발생하는데 이때 실시간으로 발생한 정보들은 공유가 불가피하다. 환자의 생체 정보는 생명과 연결되기 때문에 공유할 때 안전이 중요하다. 하지만 u-RPMS에서는 무선 통신으로 동작하기 때문에 보안에 취약하며, 이를 보안하기 위해서 서버와 DB(Data Base) 사이에 인증 서버를 통해서 해결 할 것을 제시한다. 본 연구에서는 인체 무선망을 기반으로 해서 모듈화 된 오픈 소스 원격진료 플랫폼인 OpenEMed의 개인 확인 서비스(PIDS, Personal Identification Service)를 이용해 네트워크를 기반으로 한 Kerberos 인증을 제안한다.

1. 서론

최근 가장 큰 화두인 웰빙의 관심이 음식부터 시작하여 시간이 지나면서 건강으로 중심을 옮기고 있으며 또 고령화 사회가 급속하게 진행되고 있고 건강의 문제를 중요하게 생각하여 의료 기술의 발달에 관심이 높아지고 있다. IT기술이 급속도로 발달함으로 인해 많은 분야에서 IT 기술과 융합이 이루어지고 있고 의료 분야도 마찬가지로 IT 기술과 융합되어 u-Health 서비스가 시작되었고 많은 보급화가 되지 않았지만 u-Health의 관심은 증가하고 있다[1]. u-Health 서비스의 관심이 증가됨에 따라 국내·외에서 u-Health 시장은 점점 커지고 있는데 인구의 고령화가 심해지고 u-Health 시장은 점점 더 급속도로 커질 것으로 예상된다. 그 뿐만 아니라 u-Health의 시장이 커지고 의료기관에서는 보다 빠르고 정확하게 환자를 치료하는 방법이 필요 했는데 그 방법이 환자를 치료하기 위해 인체 무선망이라는 환경을 구축하고 이를 기반으로 원격지에서 생체 정보를 전달받는 시스템이 u-RPMS(USN Remote Patient Monitoring System)이다. u-RPMS이란 환자의 생체 정보를 실시간으로 수집해서 모니터링 할 수 있는 시스템으로 본래 u-RPMS의 목적은 지속적으로 병원을 방문해야 하는 환자를 원격 모니터링 시스템을 이용해서 관리하는 것이다. 이때 u-RPMS에서는 환자의 생체 정보가 실시간으로 발생 되는데 발생한 환자의 생체 정보들은 원격 모니터링을 위해서 공유가 불가피 하다[1]. 환자의 생체 정보는 환자의 생명과 직접적으로 연결되기 때문에 환자의 생체 정보를 전달 할 때 안전이 중요 하지만 u-RPMS에서는 무선 통신을 이용해서 동작하기 때문에 보안에 매우 취약하다. 문제점을 보안하기 위해서 선행연구[1]가 진행되었지만 환자의 생체 정보 전달에만 집중했기 때문에 안전성을 강조할 필요가 있었다. 특히 실시간으로 발생한 환자의 생체 정보를 전달 할 때 인증 문제점을 보완하기 위해서 선행연구[1]에 인증 서버를 추가한다. 보다 안전하고 정확하게 환자의 생체 정보를 전달하는 인증 서버는 OpenEMed의 PIDS(Personal Identification Service)를 이용한 Kerberos를 적용한다. 2장에서는 관련연구들을 소개하고, 3장에서는 OpenEMed의 PIDS(Personal Identification Service)를 이용한 Kerberos 인증 서버를 u-PRMS에 적용시키고, 4장에서는 결론과 향후 연구내용을 제시한다.

2. 관련 연구

2.1 OpenEMed

OpenEMed 내의 서버레벨 보안은 CORBA(Common Object Request Broker Architecture)로 구현된 두개의 보안 모듈 즉, RADS(Resource Access Decision Service)와 PIDS(Personal Identification Service)에 의해 제공된다. RADS는 환자 정보에 대한 사용자 접근 권한을 관리하며, PIDS는 사용자의 인증을 제공한다. PIDS가 사용자들을 인증한 후에 RADS가 권한인가를 수행하게 된다. 데이터의 기밀성은 RSA(Rivest Shamir Adleman)알고리즘과 키 교환을 위해 디지털 인증서를 사용하는 단대단 SSL(Secure

Sockets Layer) 암호화를 사용하여 유지된다. 부인방지 정책을 강화하고 HIPPA(Health Insurance Portability and Accountability Act)제도를 만족하기 위하여 OpenEMed의 현재 버전은 PIDS에 의해 식별된 객체들에 대한 이전 정보를 관리하는 COAS(College of Oceanic and Atmospheric Sciences)에 의존하고 있다. 환자의 프라이버시를 보호하기 위하여 OpenEMed는 환자들에게 유일한 익명을 부여하여 환자들을 익명으로 처리 할 수 있도록 하고 있다. 예를 들어 환자를 보살피는 사람들은 환자 개인을 식별 할 수 있는 데이터는 제외하고 오직 자신들을 업무를 완성 할 수 있는 정도의 데이터만을 연구자들이 접근 할 수 있도록 환자 데이터들의 양과 종류를 제어하기 위하여 RADS를 사용하며 전송채널상의 데이터의 무결성은 SSL에 의해서 제공된다[2].

2.2 Kerberos 관련 연구

기존에 Kerberos 연구는 유선 네트워크 또는 PC 환경에서 이루어졌다. 그에 대한 관련 연구는 아래와 같다.

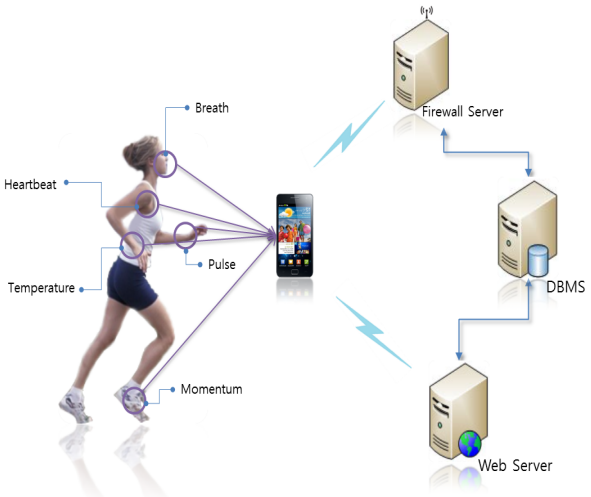
분산 네트워크 환경에서 커버로스는 시스템간의 신뢰를 바탕으로 대칭키를 사용하여 사용자를 인증한다. 그러나, 인증(authentication)과 함께 허가(authorization)는 보안의 필수적인 요소다. 본 논문에서는 기존의 커버로스에 프록시 권한 서버(proxy privilege server)를 두고 공개키/개인키를 적용하여 효율적이고 안전한 이즈 및 허가 메커니즘을 설계하였다. 제안한 메커니즘에서는 사용자 인증을 위해 미리 정해진 long-term 키와 공개키를 통해 교환한 랜덤 수에 MAC 알고리즘을 적용하여 암호화에 사용하는 세션 키 값을 매번 바꾸어주기 때문에 안전성을 높였다. 또한, 전체적인 인증 절차를 간소화하여 사용하는 키의 수를 줄였다. 프록시 권한 서버는 사용자의 권한 요구를 응용서버에 전달하고 권한 위임에 사용된다. 제안한 메커니즘을 사용하여 기존의 커버로스에서 동작하는 효율적이고 안전한 인증 및 허가 알고리즘을 설계하다[3].

Client/Server의 분산 네트워크 환경에서 Kerberos 인증 메커니즘은 Local 영역에 있는 사용자가 다른 영역에 존재하는 Kerberos 서버의 신뢰성이 있는 전제 조건에서 운용하고 있다. 하지만 Kerberos 서버간의 인증 서버의 보안 정보가 누설되면 Kerberos에 대한 신뢰성이 보장되지 않는 단점을 가지고 있다. 이런한 문제점을 해결하기 위하여 제안된 인증 메커니즘은 외부 영역 TGS에 접근하는 방법을 단순화 시켜 서비스-승인 티켓을 얻는 인증절차를 단순화 시켰다. 기존의 Kerberos 시스템을 활용할 수 있는 효율적인 방법의 인증 방법과 분할된 패스워드 사용을 통하여 패스워드 검증자의 랜덤성을 증가시켜 패스워드 추측 공격이 어렵도록 하였으며 비밀 분산 기법을 적용한 패스워드 기반 인증 방법을 사용한 인증 메커니즘이다[4].

3. 설계

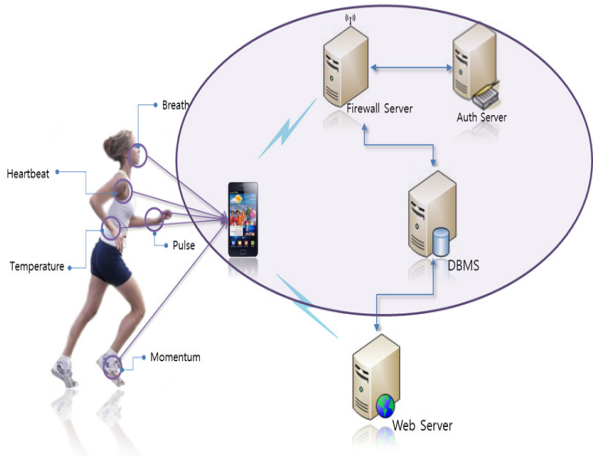
3.1 u-RPMS 모델

인체 무선망이란 USN(Ubiquitous Sensor Network)을 통해 환자의 생체 정보를 실시간으로 수집하는 시스템이다. 이를 기반으로 원격으로 환자의 생체 정보를 실시간으로 전달 받아 모니터링 하는 시스템이 u-RPMS이다. u-RPMS 모델은 (그림 1)과 같다.



(그림 1) u-RPMS 서비스 모델

(그림 1)은 환자의 생체 정보가 실시간으로 수집되어 모바일에 전달되고 그 정보가 실시간으로 수집된 정보를 Firewall Server에 무선 통신을 이용해 전달 후 전달된 환자 생체 정보는 DBMS에 저장되고 저장 된 환자 정보를 웹 서버를 이용해 모바일에서 모니터링 된 것을 보여준다. 하지만 실시간으로 환자의 생체 정보 데이터가 발생하기 때문에 사용자 인증에 대해 문제점이 있다. 그 이유는 데이터를 전달 할 때마다 인증을 해야 하는 문제가 있기 때문에 (그림 2)와 같은 시스템을 적용한다.



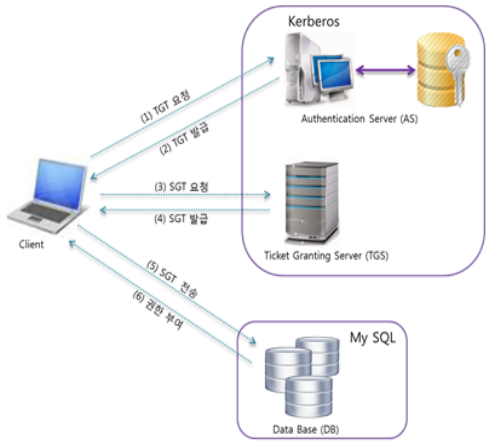
(그림 2) u-RPMS에 인증 서버를 추가 한 모델

(그림 2)는 (그림 1)에 인증 문제를 해결하기 위해서 Firewall Server와 DBMS 사이에 OpenEMed의 PIDS(Personal Identification Service)를 기반으로 한 Kerberos 인증 Server를 추가해 환자의 생체 정보를 실시간으로 전달하기 위해서 발생하는 인증 문제와 보안 문제를 해결하고 환자의 생체 정보를

효율적으로 관리한다.

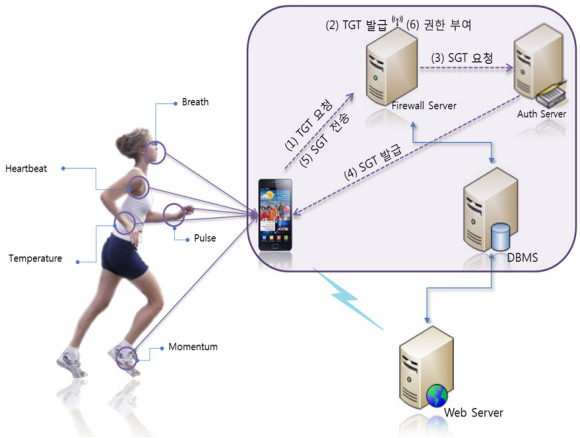
3.2 OpenEMed의 PIDS에 Kerberos적용

다음 (그림 3)은 기본적인 Kerberos 모델을 보여준다.



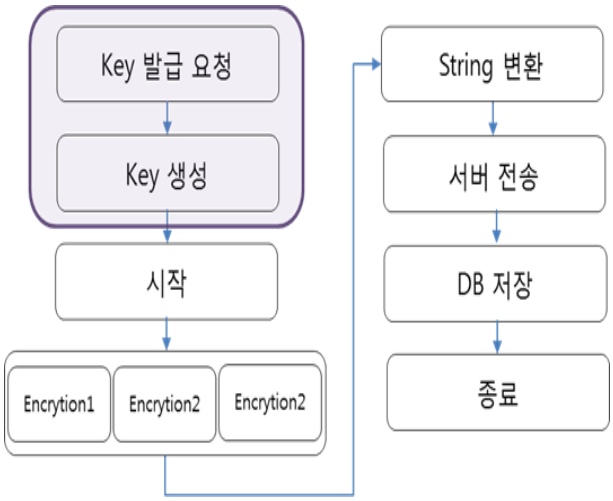
(그림 3) Kerberos 인증 서비스 모델[3]

(그림 3) Kerberos의 인증 시스템은 여러 가지 요소로 구성된 복합시스템으로 Kerberos Server와 TGS(Ticket Granting Server)가 티켓을 생성하여 TGS와 서비스 서버와의 통신에 사용되며 티켓의 구성 정보는 서버와 클라이언트 이름, 타임스탬프, 유효시간, 세션 키를 포함한다. 인증자는 클라이언트에 의해 생성되고 생성된 인증자는 사용을 1회로 제한하고 있다. (1)client가 AS(Authentication Server)에 TGT(Ticket Granting Ticket)을 요청하면 (2)AS에서 클라이언트에서 받은 정보를 통해서 알아낸 키를 가지고 TGT를 발급한다. (3)TGS에 TGT를 가지고 SGT(Server Granting Ticket)를 요청하면 (4)TGS에서 TGT를 복호화하고 client와 DB의 정보를 비교한 후 SGT를 발급한다. (5)TGS에서 받은 SGT를 전송하고 서버는 해당 자료를 비교한 후 권한을 부여한다. (6)서버에서 사용할 수 있는 권한을 승인 받는다.[5] (그림 4)는 u-RPMS에 Kerberos 인증을 적용한 모델이다.



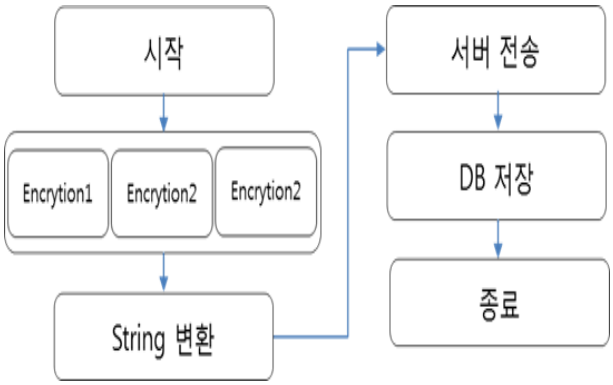
(그림 4) u-RPMS에 Kerberos 인증 적용 모델

(그림 4)와 같이 시스템을 적용하여 모바일을 클라이언트로 Firewall Server에 AS를 적용시키고 TGS를 적용시켜서 모바일에서 직접 키를 발급 받는 방식을 적용시킨다. 최초 인증 시에 Key의 값을 부여 받아서 인증을 지속하게 된다. 최초 인증 시에 (1)부터 (4)를 포함하여 인증을 하고 인증 후는 (5)와 (6)만을 반복하게 된다. (그림 5)는 Client 측 흐름도를 보여준다.



(그림 5) client 측 흐름도 (최초 동작)

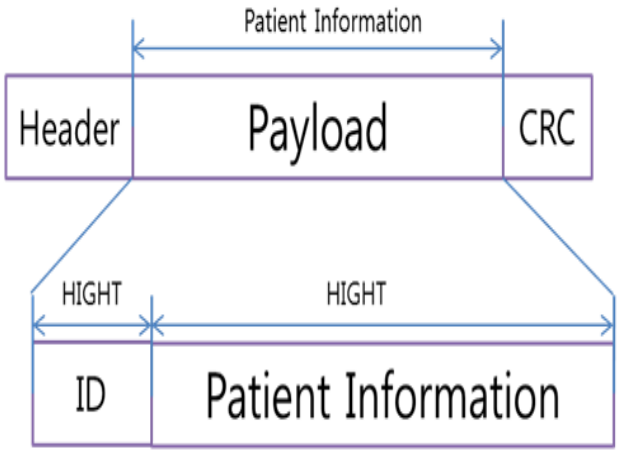
(그림 5)는 client측에서 최초 동작 시 흐름도를 보여주는데 먼저 모바일에서 Firewall Server로 TGT를 요청하면 Firewall Server에서 TGT를 발급하고 발급한 TGT를 가지고 TGS에 SGT를 요청한다. TGS에서 SGT를 모바일에 발급을 하고 모바일에서 최초 동작 후 SGT에서 발급한 Key 값을 보유하게 된다.



(그림 6) client 측 흐름도 (최초 동작 후)

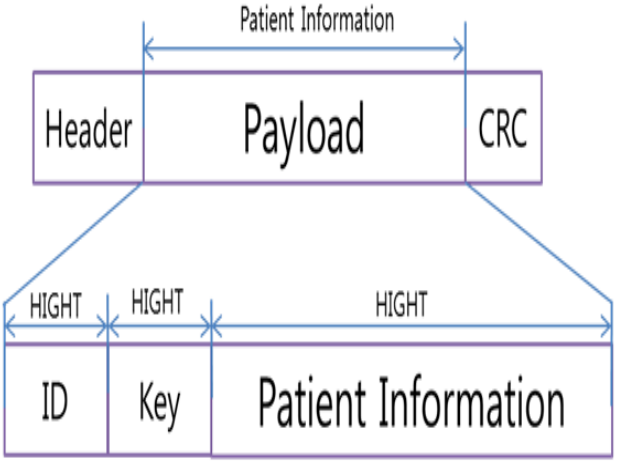
(그림 6)은 최초 동작 후의 흐름도를 보여주는데 최초 동작 시에 Key의 값을 발급 받아 모바일에서 Key의 값을 보유 하고 있기에 보유하고 있는 Key의 값을 환자의 정보에 추가해서 Firewall Server에서 인증 받고 권한을 부여 받으면 DBMS에 환자의 생체정보만을 저장하게 된다.

이 때 발급 받은 Key의 값을 추가하고 이용하는 문제가 생기게 된다. 이것을 해결하기 위해서 HIGHT 암호화를 단계별로 나누어서 암호화한다. (그림 7)은 HIGHT 암호화를 2단계 한 구성도이다.



(그림 7) HIGHT 암호화 2단계 적용

(그림 7)은 HIGHT 암호화 2단계로 적용한 모습인데 환자의 정보와 생체 정보를 따로 암호화 하여서 인증 할 때 환자의 정보만을 복호화하여 인증 Key값을 요청하는데 사용하게 된다. Key값을 처리하기 위해서 본 연구에서는 발급 받은 Key 값을 추가해 HIGHT 암호화를 한다. 다음은 HIGHT 암호화를 3단계로 적용한 것이다.



(그림 8) HIGHT 암호화 3단계 적용

(그림 8)은 발급 받은 Key 값을 전달할 데이터에 추가해서 환자의 정보, Key 값, 환자의 생체 정보를 나누어 HIGHT 암호화를 하여 최초 인증 시에 ID 값을 복호화하고 인증 후에 Key 값을 복호화해서 인증을 받아 권한을 부여 받고 환자의 생체 정보만 DBMS에 저장하게 설계하였다.

4. 결론 및 향후 연구

본 연구에서는 인체 무선망 기반으로 한 u-RPMS에서 실시간으로 발생한 환자의 생체 정보 전달을 안전하고 정확하게 전달하기 위해서 Firewall Server와 DBMS사이에 인증 서버를 추가하여 안전성을 보완한다. 사용한 서버는 모듈화된 오픈 소스 원격진료 플랫폼인 OpenEMed의 개인 확인 서비스 PIDS를 이용해 네트워크를 기반으로 한 kerberos 인증 서버를 적용 하는 것을 제안하였다. 향후 연구에는 본 논문에서 설계한 모델의 적합성 및 성능 검증을 위해서 CentOS에서 kerberos를 구축하고 기존 방식과 비교 평가를 위해 데이터 payload가 분리된 형태의 encryption 인증키 값과 non-encryption 인증키 값의 인증절차에 대한 실험을 수행할 예정이다.

"이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0013029)"

참고문헌

[1] Young-Hyuk Kim "A Study on Security Model for Secure Biometric Information of BAN", Feb, 2011

[2] 한국정보보호진흥원 "원격 의료용 바이오 인증 기술 침 표준 개발" 최종연구보고서 (KISA-WP-2007-0054) 2007.12.

[3] 김은환, 김명희, 전문석 "커버로스 기반의 안전한 인증 및 허가 프로토콜에 관한 연구"한국통신학회, 한국통신학회논문지, 제29권 5C호 2004.5, page(s): 737-749

[4] 조경옥, 김종우, 하태진 한승조 "분산 네트워크 환경에서 분할 password를 이용한 Kerberos 인증 메커니즘 설계" 대한전자공학회, 대한전자공학회 2004년 하계종합학술대회 2004.6, page(s): 761-766

[5] 김철현, 이연식 "Kerberos 인증메커니즘에 관한 연구" 한국정보보호학회, 정보보호학회논문지, 제15권 제3호 2005.6, page(s): 53-64