바이오 인증을 사용한 원격의료시스템의 취약성 분석 및 대응방안

정회원 황 유 동*, 이 유 리*, 박 동 규*, 신 용 녀**

Vulnerability Analysis and Countermeasure of Telemedicine System Using Bio-Authentication

Yu-dong Hwang*, You-ri Lee*, Dong-gue Park*, Yong-Nyuo Shin** ***Regular Members***

요 약

본 논문에서는 바이오 인증을 사용한 안전한 원격의료 시스템 모델을 제시한다. 안전한 시스템 모델을 생성하기 위해 다양한 원격의료 시스템 서비스 시나리오와 각 서비스의 프로세스를 분석하였다. 또한 바이오 인식 원격의료 시스템의 안전한 서비스 제공을 위하여 제시한 모델의 보안 취약성 및 위협을 분석하고 각 위협에 대한 대응책을 제시하였다. 본 논문의 결과는 원격 바이오 인증을 사용하는 원격진료 시스템의 개발을 위한 표준 문서로 효율적으로 사용될 수 있다.

Key Words : Telebiometric, Telemedicine, Bio-Authentication

ABSTRACT

This study is to propose model for secure telemedicine system using bio-authentication. In this paper, we analyze various processes and scenarios for telemedicine service in order to create functional model of it. Also, we analyze the vulnerabilities and threats of the proposed model and make countermeasures for each threat in order to suggest secure service of telemedicine system based on biometric. The results of this study is effectively used as stadard documents for development of telemedicine system using telebiometrics.

Ⅰ. 서 론

최근 국내에서는 첨단 IT인프라와 유비쿼터스 정보 서비스를 도시 공간에 융합하여 생활의 편의 증대와 삶의 질 향상, 체계적 도시 관리에 의한 안전 보장과 시민복지 향상, 신산업 창출 등 도시의 제반 기능을 혁신시키는 차세대 정보화 도시인 "U-City"를 중앙정부의 정책적 지원 아래 지방 자치 단체와 통신사업자, 건설 사업자, SI/NI 사업자 등이 중심이 되어 추진하고 있다. "U-City"는 국내의 발전된 정보 기술의 역량이 총체적으로 결집되고 건설, 가전, 문화, 의료 등의 융합을 실현하는 21세기 한국형 신도시를 뜻한다. "U-City"의 서비스들은 다양한 연구가 진행되고 있으며, 서비스 들 중 대표적인 서비스는 홈 네트워크와 텔레메틱스, 원격의료 서비스 등이 있으며, 그 중에서도 원격의료 서비스는 삶의 질 향상에 밀접한 관련이 있는 서비스 이다.[8,9]

원격의료 서비스는 개인의 생명에 영향을 주는 기능을 서비스함으로써 악의적인 목적을 가진 공격자가 원격의료 서비스에 대한 불법적인 공격으로 개인의 프라이버시 침해뿐만 아니라, 생명 및 재산

* 순천향대학교 정보통신공학과 (hwangyudong@gmail.com, thisglass@sch.ac.kr, gpark@sch.ac.kr)
** 한국정보보호진흥원 보안성평가단 산업지원팀 (ynshin@kisa.or.kr)
논문번호 : 07106-1220, 접수일자 : 2007년 12월 20일

에 까지 직접적인 피해를 줄 수 있으므로, 원격의료 서비스가 성공적으로 수행되기 위해서는 초기단계에서부터 반드시 보안기술을 고려해야 한다.[1-7]

즉, 원격의료 서비스 관련 인프라를 안전하게 운영할 수 있는 보안기술이 적용되어야 하며, 이와 더불어 다양한 보안 위협으로부터 안전하게 원격의료 서비스를 제공할 수 있어야 한다. 이를 위해서는 각 서비스별 보안 위협 또는 취약점을 분석하고 보안 요구 사항을 도출해서 필요한 보안 기술을 적용해야 한다.

본 논문에서는 2장에서 원격의료 서비스의 취약점과 대응방안을 정리하고, 3장에서 바이오 인증을 사용한 원격의료 서비스의 시나리오를 정의하고, 4장에서는 3장에서 정의된 시나리오를 기반으로 한 원격의료 서비스의 프로세스를 정의하였다. 5장에서는 원격의료 서비스의 프로세스를 기반으로 보안 취약점 분석 및 대응방안을 도출하고 6장에서 결론을 맺는다.

Ⅱ. 원격의료 서비스 취약점과 대응방안

원격의료 서비스의 보안상 취약점은 다른 온라인 서비스들과 마찬가지로 다양한 취약점들이 존재하며, 원격의료 서비스에 사용되는 새로운 장비들과의 네트워크에서 존재하는 신규 취약점이 존재하고 대표적인 보안 침해 유형은 다음의 네가지이다.[9]

1) 네트워크상에서 패킷을 캡처(Capture)하여 패스워드, 중요 데이터 및 특정 서비스 기능에 관련된 정보를 도청하여 수집한다.[9]
2) 프로토콜의 취약점을 이용(IP Spoofing, Prediction 등)하여 정당한 사용자나 시스템으로 신분 위장하여 각종 게이트웨이를 공격한다.[9]
3) 게이트웨이나 무선AP를 대상으로 네트워크 사용량을 초과 하도록 대량의 메일을 보내거나 다량의 무선랜 접속 요구를 통해 서비스거부 공격을 한다.[9]
4) 서비스의 사용량 수집 및 개인 정보 수집을 통한 프라이버시 침해를 목적으로 하는 정보 수집이 있다.[9]

위에서 나열한 네가지의 침해 유형에 따른 기존의 대응방안은 인증 프레임워크 메커니즘을 통한 다단계 서비스 접근인증을 통한 방법과, 기기 및 사용자 인증 메커니즘을 이용한 대응방안이다. U-HC 디바이스를 이용한 서비스 이용 시 서버나 게이트웨이 접근 시 U-HC 기기와 서로 인증을 통한 서비스 허용 방법, 인프라 기반의 다양한 대응 방안인 서비스 액세스의 우선순위 지정과 같은 엄격한 인증 및 접근제어 방안, 불법 접근 공격을 방어하기 위하여 기밀성을 제공하는 암호화 기법, 도난, 분실, 복제, 도청에 따른 인증 강화 대책이 필요하며 바이러스/웜, 해킹, 위/변조 공격에 대응하기 위하여 방화벽, VPN 등의 방어기술 및 보안이 강화된 인증 방법 도입이 있다.[8,9]

본 논문에서는 이중에서도 특히 인증 방식에 대한 인증 서비스 신뢰성을 보장하기 위한 방안으로 바이오 정보를 이용한 사용자 인증과 암호화 기법을 적용한 원격의료 서비스 시나리오와 프로세스를 제시한다.

Ⅲ. 원격의료 서비스 시나리오

원격의료 서비스는 다양한 상황과 환경에서 의료정보에 접근을 가능하게 한다. 다음 그림 1, 2, 3, 4, 5, 6은 원격의료 서비스의 시나리오 예이다.

그림 1은 응급 상황 발생 시의 시나리오이다.

그림 1의 시나리오는 다음과 같다.

① 응급환자 발생 시 환자의 진료 기록을 열람하는 의사는 인증을 받기위하여 인증 정보를 의료정보 시스템으로 전송한다.

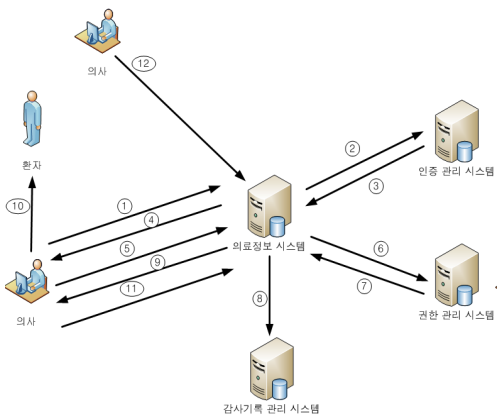

그림 1. 원격의료 서비스 시나리오 예 1

② 의료정보 시스템은 전송된 의사의 인증 정보를 이용하여 인증 관리시스템에 인증여부를 확인한다.

③ 인증 관리 시스템으로부터 전송된 인증 확인 메시지를 ④ 인증을 요청한 의사에게 전송한다.
⑤ 인증된 의사는 환자의 정보를 전송하여 환자의 진료 정보를 요청한다.
⑥ 환자의 정보와 함께 전송된 의사의 권한 정보를 이용하여 권한 관리 시스템에 권한을 확인한다.
⑦ 권한 관리 시스템으로부터 권한이 확인되면 ⑧ 감사기록 관리 시스템에 의사의 환자 정보 열람에 대한 기록을 갱신하고 ⑨의사에게 환자에 대한 진료 정보를 전송한다.
⑩ 의사는 전송된 환자의 진료 정보를 확인하여, 진료 및 처방을 하고, ⑪ 진료 및 처방 정보를 의료 정보 시스템으로 전송한다.
⑫ 다른 의사로부터 진료 및 처방에 대한 정보를 받아야 하는 경우 상대방 의사는 동일한 인증체계를 거친 후 메시지를 송수신한다.

다음 그림 2의 시나리오는 환자가 원격의료 서비스를 제공받기 위하여 의료 기관 또는 보험 서비스 기관에 등록하는 시나리오의 예이다.
그림 2의 시나리오는 다음과 같다.

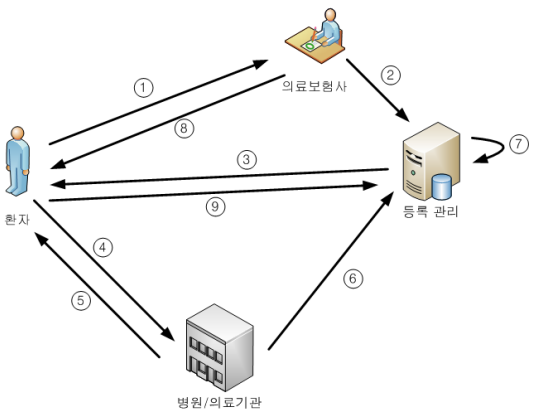

그림 2. 원격의료 서비스 시나리오 예 2

① 환자는 등록을 위하여 등록 양식을 작성하여 제출한다.
② 제출된 환자의 등록 양식을 검사한 후 ③ 환자에게 의료검사 일정을 통보한다.
④ 환자는 예정된 의료 검사 일정에 따라 의료 검사를 실시하고 ⑤ 의료 검사 결과를 통보 받는다.
⑥ 환자의 의료검사 결과는 등록기관에도 통보된다.
⑦ 등록기관에서는 환자를 등록하고, ⑧ 원격의료 서비스관련 계약서를 전송한다. ⑨ 등록된 환자는 향후 사용자 인증을 한후 원격의료 서비스를 요청하고 제공받는다.

다음 그림 3의 시나리오는 환자로부터 수집된 의료 데이터를 이용하여 시험된 결과를 의사에게 전달하고 시험된 결과를 기반으로 환자가 의사의 진료를 받게되는 시나리오이다. 그림 3의 시나리오는 다음과 같다.

① 환자로부터 의료 데이터를 수집하여 시험소로 전송한다.
② 시험소는 시험 결과를 건강 관리기관에 전송한다.
③ 건강관리 기관은 검사결과가 나왔음을 의사에게 통보하고, ④ 의사는 건강관리기관에 인증을 요청하고, 환자의 검사 결과 정보를 요청한다.
⑤ 건강관리기관은 의사에게 환자의 검사 결과를 전송하고 ⑥ 의사는 검사결과를 기반으로 소견서를 작성하여 ⑦ 건강관리기관으로 소견서를 전송하면, ⑧ 건강관리기관은 의료정보관리 시스템에 데이터를 갱신 한 후 ⑨ 환자에게 서비스를 제공한다.

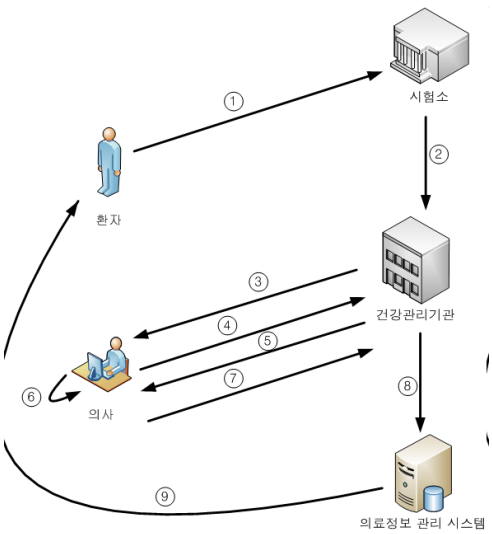

그림 3. 원격의료 서비스 시나리오 예 3

다음 그림 4의 시나리오는 환자와 의사의 치료 상담 시나리오이다. 그림 4의 시나리오는 다음과 같다.

① 환자가 의사 웹사이트에 인증 및 상담을 요청

한다. ② 의사 웹 사이트는 환자의 인증을 확인한 후 ③ 의사에게 응답을 요청하고, ④ 의사로부터 서명된 응답 메시지를 전송받는다.
⑤ 환자로부터 다시 인증과 의사의 응답 메시지를 요청받으면, ⑥ 저장된 의사의 응답메시지를 환자에게 제공한다.

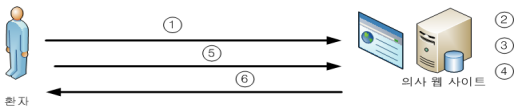

그림 4. 원격의료 서비스 시나리오 예 4

다음 그림 5의 시나리오는 환자에게 의료서비스를 제공하기 위한 시나리오이다. 그림 5의 시나리오 설명은 다음과 같다.

① 의료 서비스 제공소는 다른 의료 정보 관리 시스템과 상호 인증하여 의료 정보를 수집한다.
② 환자의 리포트를 작성한다.
③ 작성된 환자의 리포트를 의사의 검수 및 검토를 받는다.
④ 감사 기록정보를 갱신한다.
⑤ 환자는 의료 서비스를 제공받기 위하여 인증을 요청한다.
⑥ 환자를 인증한 후 ⑦ 환자의 서비스 요청이 있으면, ⑧ 서비스를 제공한다.

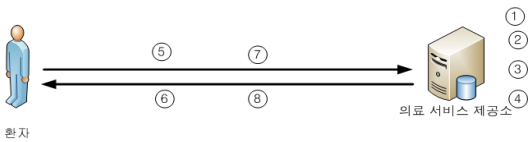

그림 5. 원격의료 서비스 시나리오 예 5

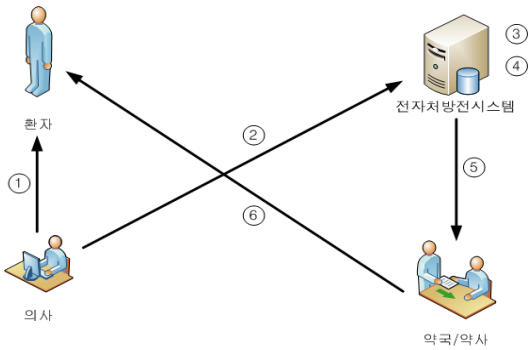

그림 6. 원격의료 서비스 시나리오 예 6

위 그림 6의 시나리오는 환자의 진료 후 환자를 위한 전자처방전에 대한 시나리오이다. 그림 6의 시나리오는 다음과 같다.

① 의사는 환자를 진찰한 후 ② 의사의 서명과 함께 전자처방 정보를 전자처방전 시스템으로 전송한다. ③ 전자처방전 시스템은 의사의 인증서를 확인한 후 ④ 처방전을 검토하여, ⑤ 처방전을 발행한다. ⑥ 약사는 환자에게 처방전에 맞는 약을 제공한다.

Ⅳ. 원격의료 서비스 프로세스

원격의료 서비스는 개인의 생명과 직접적인 관련이 있는 기능을 서비스함으로써 불법적인 공격으로 개인의 프라이버시 침해뿐만 아니라, 생명 및 재산에 직접적인 피해를 줄 수 있으므로, 기존의 보안 시스템에서 제공하는 일반적인 사용자 인증 방법보다 분실 및 도용 등으로부터 상대적으로 안전한 바이오 정보를 이용한 인증을 사용한다.

4장에서는 3장에서 예를 보인 원격의료 서비스 시나리오를 기반으로 원격의료 서비스 프로세스를 정의하였다. 2장의 원격의료 서비스 시나리오에서 알 수 있듯이 원격의료 서비스 프로세스는 사용자(서비스 대상자, 서비스 제공자) 등록, 서비스 대상자(환자)의 의료 정보 데이터 송, 수신과 서비스 제공자(의사, 약사, 보험관리자 등)의 데이터 송, 수신으로 나눌 수 있다.

다음 그림 7은 원격의료 시스템에서 환자의 데이터를 수집하는 프로세스이고 다음 그림 8은 환자가 진료기록, 처방전, 의사의 상담 내용 등의 의료 정보를 요청하는 프로세스이다.

그림 7과 8에서 알 수 있듯이 환자가 원격의료 서비스를 제공받기 위해서는 반드시 사용자 인증이 되어야 하고, 또한 권한이 관리 되어야 한다.

다음 그림 9는 의사의 의료정보 송, 수신 프로세스이고, 다음 그림 10은 원격의료 서비스 사용자 등록이다.

3장에서 설명한 원격의료 서비스 시나리오에서 그림 1의 응급 상황 발생시의 시나리오는 그림 9의 의사의 의료정보 송, 수신 프로세스를 적용할 수 있고, 그림 2의 원격의료 서비스 기관에 사용자 등록 시나리오는 다음 그림 10의 사용자 등록 프로세스를 적용할 수 있다.

그림 3의 시나리오는 그림 7 환자의 의료정보 송

신 프로세스와 그림 9 의사의 의료 정보 송, 수신 프로세스를 적용할 수 있다. 그림 4, 5, 6의 시나리오 또한 그림 7, 8, 9의 프로세스를 적용할 수 있다. 또한 그림 7, 8, 9의 프로세스는 중복되는 기능을 표현하므로 하나의 프로세스로 표현이 가능하다. 다음 그림 11은 다음 그림 7, 8, 9의 프로세스를 하나의 프로세스로 표현한 것이다. 그림 11에서 실선은 환자의 의료 정보 데이터 송, 수신 프로세스이고, 점선이 의사의 의료 정보 데이터 송, 수신 프로세스이다.

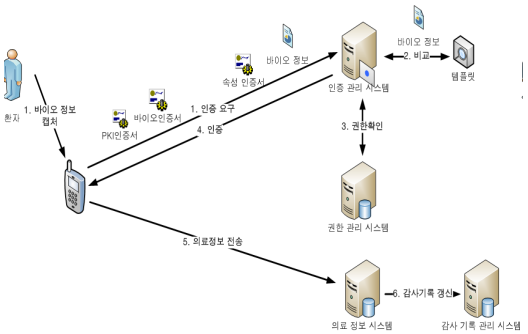

그림 7. 환자의 의료 정보 송신 프로세스

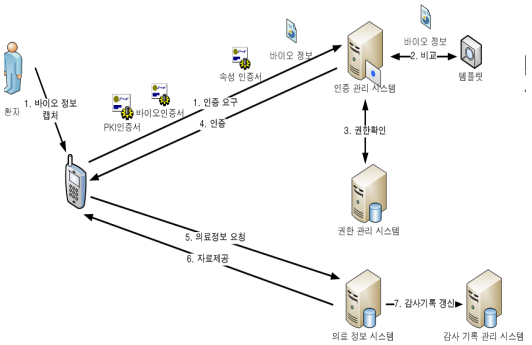

그림 8. 환자의 의료정보 전송, 수신 프로세스

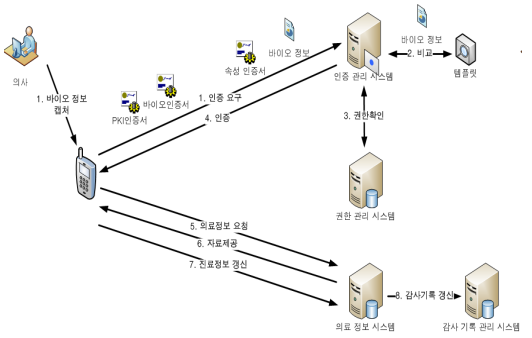

그림 9. 의사의 의료정보 송, 수신 프로세스

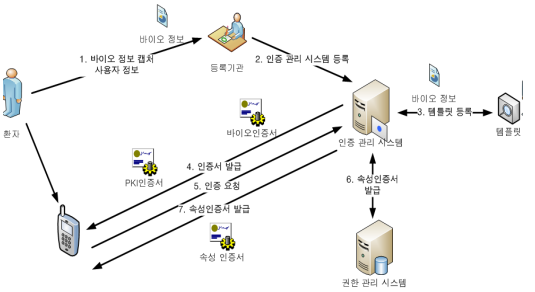

그림 10. 사용자 등록 프로세스

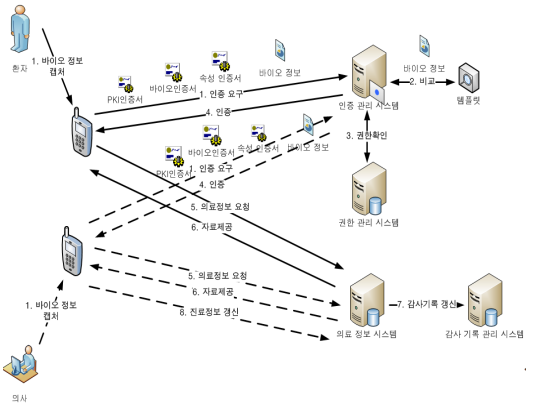

그림 11. 환자, 의사의 의료정보 송, 수신 프로세스

V. 원격의료 시스템의 보안위협과 대응책

다음 그림 12는 원격의료 시스템의 기능 모델과 취약점을 분석한 것이다. 원격 의료시스템에서도 다음 그림 12와 같이 다양한 보안 취약점과 위협 요소들이 존재하며, 유무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점 및 공격이 원격 의료 시스템 환경에서도 유사하게 발생되는 형태를 보인다. 따라서 원격 의료 시스템의 기반 네트워크 및 시스템에 대한 안전성, 신뢰성 보장 및 데이터 보호를 위한 정보보호 기술의 개발이 절실히 필요하다.[8-10]

본 장에서는 위 그림 10의 사용자 등록 프로세스와 그림 11의 환자, 의사의 의료정보 송, 수신 프로세스에서 보안 취약점을 분석하고, 대응책을 제시한다.

다음 그림 12의 원형 번호는 기능 모델의 취약점을 표시한 것으로 원격의료 시스템의 기능 모델에서 모든 모듈과 통신로에 보안위협은 존재하며, 보안위협 1~43 까지의 각 위협에 대한 설명은 다음과 같다.

1) 바이오 템플릿 입력장치에 대한 공격

2) 바이오 샘플을 바이오 템플릿 추출부로 전송하는 과정에 대한 공격
3) 바이오 템플릿 추출부에 대한 공격
4) 추출된 바이오 템플릿을 인증 정보 등록 모듈과 인증 모듈로 전송하는 과정에 대한 공격,
5) 등록부에 대한 공격
6) 등록부에서 사용자 정보 DB로 전송하는 과정에 대한 공격
7) 사용자 정보 DB에 대한 공격
8) 등록부에서 인증 정보 등록 모듈로 전송하는 과정에 대한 공격
9) 인증 및 인가 정보 등록 모듈에 대한 공격
10) 인증 및 인가 정보 등록 모듈과 PKI 인증 정보 등록 모듈의 전송로에 대한 공격
11) PKI 인증 정보 등록 모듈에 대한 공격
12) PKI 인증 정보 등록 후 생성된 인증서를 인증서 디렉토리에 전송하는 과정에 대한 공격
13) PKI 인증서 디렉토리에 대한 공격
14) PKI 인증 정보 등록 모듈에서 바이오 인증 정보 등록 모듈로 전송하는 과정에 대한 공격
15) 바이오 인증 정보 등록 모듈에 대한 공격
16) 바이오 인증 정보 등록 모듈에서 바이오 템플릿 등록 모듈로 전송하는 과정에 대한 공격
17) 템플릿 등록 모듈에 대한 공격
18) 템플릿 등록 모듈에서 바이오 정보 템플릿 저장 DB로의 템플릿을 전송하는 과정에 대한 공격
19) 바이오 정보 템플릿 DB에 대한 공격
20) 바이오 인증 정보 등록에서 권한 인증 정보 등록으로 전송하는 과정에 대한 공격
21) 권한 인증 정보 등록 모듈에 대한 공격
22) 권한 인증 정보 등록 모듈에서 속성 인증서 디렉토리로 전송하는 과정에 대한 공격
23) 속성 인증서 디렉토리에 대한 공격
24) 인증 및 인가 모듈에 대한 공격
25) 인증 및 인가 모듈과 PKI 인증서 관리 모듈로 전송하는 과정에 대한 공격
26) PKI 인증서 관리 모듈에 대한 공격
27) PKI인증서 관리 모듈과 인증서 디렉토리 사이의 데이터 전송과정에 대한 공격
28) PKI인증서 관리 모듈과 바이오 인증서 관리 모듈 사이의 전송 과정에 대한 공격

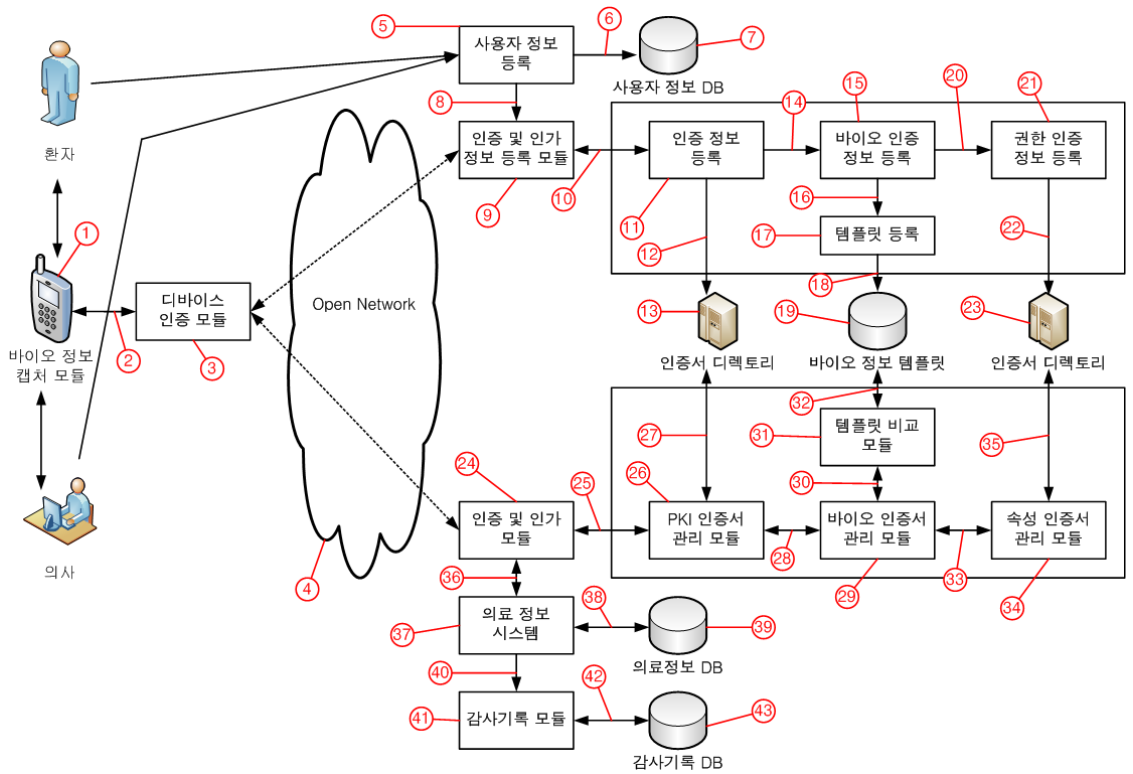

그림 12. 원격의료 시스템 기능 모델과 취약점

29) 바이오 인증서 관리 모듈에 대한 공격
30) 바이오 인증서 관리 모듈과 템플릿 비교 모듈 사이의 전송 과정에 대한 공격
31) 템플릿 비교 모듈에 대한 공격
32) 템플릿 비교 모듈과 바이오 정보 템플릿 DB 사이의 전송 과정에 대한 공격
33) 바이오 인증서 관리 모듈과 속성 인증서 관리 모듈 사이의 전송 과정에 대한 공격
34) 속성 인증서 관리 모듈에 대한 공격
35) 속성 인증서 관리 모듈과 속성 인증서 디렉토리 사이의 전송 과정에 대한 공격
36) 인증 및 인가 모듈과 의료 정보 시스템 사이의 전송 과정에 대한 공격
37) 의료 정보 시스템에 대한 공격
38) 의료 정보 시스템과 의료 정보 DB 사이의 전송과정에 대한 공격
39) 의료 정보 DB에 대한 공격
40) 의료 정보 시스템과 감사 기록 모듈 사이의 전송과정에 대한 공격
41) 감사기록 모듈에 대한 공격
42) 감사기록 모듈과 감사기록 DB 사이의 전송 과정에 대한 공격
43) 감사기록 DB 에 대한 공격

위 그림 12의 보안위협 1)~43) 중 일부 보안 위협은 telebiometrics 표준 X.tpp의 보안 위협과 밀접한 관계가 있으며, 원격의료 시스템의 보안위협과 X.tpp의 관계는 다음과 같다.[10]

- 보안위협 1)은 X.tpp의 T1과 동일하다.
- 보안위협 2)는 X.tpp의 T2와 동일하다.
- 보안위협 3)은 X.tpp의 T3과 동일하다.
- 보안위협 4), 6), 8), 14), 16), 28), 30)는 X.tpp의 T4에 포함된다.
- 보안위협 5)는 X.tpp의 T9와 포함된다.
- 보안위협 7), 17)은 X.tpp의 T6에 포함된다.
- 보안위협 9)는 X.tpp의 T9에 포함된다.
- 보안위협 15), 19)는 X.tpp의 T6에 포함된다.
- 보안위협 18), 32)은 X.tpp의 T7에 포함된다.
- 보안위협 31)은 X.tpp의 T5에 포함된다.

X.tpp와 관계없는 나머지 보안위협은 기존의 네트워크에서도 존재하는 보안위협이다.

위 그림 12에서 보안위협 10), 12), 20) 22), 24), 25), 27), 29), 33), 35), 36), 38), 40), 42) 에 해당하는 네트워크 통신로상의 보안 취약점은 물리적으로 가까거나 동일한 네트워크 환경 내에 위치하여 위협에 노출이 되지 않으면 적용하지 않아도 된다.

또한, 11), 13), 21), 23), 24), 26), 29), 34), 37), 39), 41), 43) 와 같은 시스템에 대한 보안 위협은 시스템 보안을 적용할 수 있다.

위와 같은 1)~43)의 보안 취약점에 대한 대응책은 다음과 같다.

- 바이오정보 캡처 장치의 디바이스 인증 : 외부의 다른 사람에 의해 대체되었는지 아닌지 여부를 알 수 있어야 하며, 인가되지 않는 불법 장치가 사용되는 것을 막을 수 있어야 한다. 또한 현재 사용되고 있는 장치가 정상적으로 동작하고 있는지 여부를 언제나 시험할 수 있는 특성을 구현함으로써 장치의 오동작을 감지할 수 있어야 한다.
- 바이오 정보와 공개키 알고리즘을 이용한 사용자 인증 : 사용자 인증을 통하여 인증되지 않은 비정상 사용자가 시스템에 접근할 수 없도록 하고, 사용자 인증 후 안전한 통신 경로 확보를 위한 비밀키의 전송에도 사용된다.
- 속성 인증서를 이용한 사용자 권한 관리. : 원격의료 시스템의 정보 및 서비스에 대한 접근 권한 정책을 구현 함으로써 서비스 이용단계에서부터 사용자의 권한에 맞는 접근을 허용한다.
- 비밀키 알고리즘을 이용한 안전한 통신로 확보 : 사용자 인증 후 데이터의 안전한 송, 수신을 위하여 사용된다.
- 부인봉쇄 : 디지털 서명과 감사기록과 더불어 환자의 원격의료 시스템 액세스와 의사의 액세스에 대한 확인을 위해 사용된다.
- 프라이버시 보호를 위한 디지털 서명, 권한 제어 : 의사의 진료 및 처방 등 환자의 프라이버시와 생명에 위협을 가할 수 있는 정보의 생성자와 이용자를 확인하고, 인증된 사용자에게 허가된 권한 만을 이용할 수 있도록 한다.
- 감사기록 : 원격의료 시스템의 정보 접근에 대한 모든 로그를 기록 함으로써 프라이버시 및 부인봉쇄 등에 이용된다.
- 시스템 보안 : 전통적인 시스템의 보안위협에 대비할 수 있도록 한다.

Ⅵ. 결 론

본 논문에서는 첨단 IT인프라와 유비쿼터스 정보서비스를 도시 공간에 융합하여 생활의 편의 증대와 삶의 질 향상, 체계적 도시 관리에 의한 안전 보장과 시민복지 향상, 신산업 창출 등 도시의 제반 기능을 혁신시키는 차세대 정보화 도시인 “U-City” 서비스 중에서 삶의 질 향상과 밀접한 관련이 있는 원격의료 시스템의 서비스 시나리오와 프로세스를 분석하였다. 분석된 시나리오와 프로세스를 원격의료 시스템에 적용하여 보안취약점을 분석하고 안전한 원격의료 서비스를 위한 대응책을 제시하였다. 본 논문에서 분석한 보안취약점과 제시한 대응책은 원격의료 시스템 보안을 위한 표준 제정에 기여할 것으로 사료되며, 향후 다양한 환경과 상황에서 원격의료 서비스를 위한 시나리오 및 프로세스에 대한 연구와 이에 대한 원격의료 시스템 구현이 필요한 것으로 사료된다.

참 고 문 헌

〔1〕〔Drake Patrick Mirembe, 2006〕, “Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services”, Master Thesis, Radboud University Nijmegen, July 2006.

〔2〕 http://www.ipath.ch/site

〔3〕 http://www.openemed.org

〔4〕〔Bludau & Koop, 2002〕 H. Bludau and A. Koop, editors. Mobile Computing in Medicine, Second Conference on Mobile Computing in Medicine, Workshop of the Project Group MoCoMed, GMDS-Fachbereich Medizinische Informatik & GI-Fachausschuss 4.7, 11.4.2002, Heidelberg, volume 15 of LNI. GI, April 2002.

〔5〕 http://www.ece.uah.edu/ jovanov/whrms/

〔6〕 http://www.eecs.harvard.edu/ mdw/proj/codeblue/

〔7〕〔Apollohospitals, 2006〕 Apollohospitals. http://www.apollohospitals.com, March 2 2006.

〔8〕 송지은 외,“ u-헬스케어 보안 이슈및 기술 동향”, 전자통신 동향분석 제 22권 제 1호 2007년 2월

〔9〕 김재성, 김영준, “바이오 정보를 이용한 U-HealthCare 인증방안 연구”, 한국 정보보호학회지 제 17권 제 1호 2007년 2월

〔10〕 정윤수 외,“Telebiometric 융합 기술 및 국제 표준화 동향”, TTA Journal No. 112

황 유 동 (Yu-dong Hwang) 정회원

1998년 2월 순천향대학교 제어계측 공학과 공학사

2000년 8월 순천향대학교 전기전자공학과 석사

2003년~현재 순천향대학교 전기전자공학과 정보보호전공 박사과정

<관심분야> 네트워크 보안, 시스템 보안, 접근제어

이 유 리 (You-ri Lee) 정회원

2002년 2월 순천향대학교 정보통신공학과 공학학사

2004년 2월 순천향대학교 정보통신공학과 공학석사

2004년~현재 순천향대학교 정보통신공학과 박사과정

<관심분야> 접근제어, 보안

박 동 규 (Dong-Gue Park) 정회원

1992년 한양대학교 대학원 전자공학과 공학박사

1999~2003년 순천향대학교 정보기술공학부 부교수

2004년~현재 순천향대학교 정보통신공학과 교수

<관심분야> 네트워크 보안, 유비쿼터스 컴퓨팅 보안

신 용 녀 (Yong-Nyuo Shin) 정회원

1999년 2월 숭실대학교 컴퓨터과학과 학사

2001년 9월 고려대학교 컴퓨터과학과 석사

2002년 1월~현재 한국정보보호진흥원 산업지원팀 연구원

<관심분야> 바이오인식, 정형기법, 정보보호