u-Healthcare 서비스의 정보보호 위협 분석[1)]

신동훈○, 한병진, 이환진, 정현철
한국인터넷진흥원
dhshin, bjhan, lhj79, hcjung@kisa.or.kr

Analysis of Security Threat in u-Healthcare Service

DongHoon Shin, Byoung-Jin Han, HwanJin Lee, Hyun-Chul Jung
Korea Internet and Security Agency

요 약

유비쿼터스 기술의 발전으로, u-City, u-물류, u-기상관측,u-Healthcare 등 다양한 융합 서비스가 개발되어 실생활에 적용되기를 기다리고 있다. 이들 중, 기존 의료서비스에 유비쿼터스 기술을 접목하여 언제, 어디서나 보건의료서비스를 제공하고자 하는 u-Healthcare 서비스의 경우에는, 바이오정보를 포함한 개인정보와 의료정보를 다루기 때문에 해킹으로 인한 정보유출 사고발생시 국가적인 혼란과 사회적인 불신을 야기할 수 있다. 본 논문에서는 국내외에서 추진하고 있는 u-healthcare 서비스 현황을 조사하고, 이에 대한 보안위협을 제시하여 u-Healthcare 서비스의 정보보호 대책 수립시 활용할 수 있도록 제시한다.

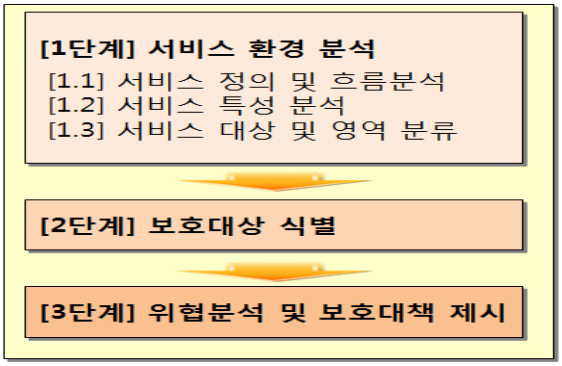
1. 서 론

u-Healthcare는 ubiquitous Healthcare의 줄임말로서, 보건의료에 유비쿼터스IT를 도입하여 환자가 병원을 찾지 않더라도 언제, 어디서나, 진단, 치료, 사후관리를 받을 수 있는 의료서비스를 말한다 나아가 환자가 아니더라도 사전진단을 통해 질병예방이 가능한 보건의료서비스의 제공을 가능하게 한다 이러한 u-Healthcare는 인터넷, BT와 IT의 Convergence인 BIT 등 정보통신 기술의 접목으로 다양하고 다변화된 의료서비스로 발전되고 있으며, 유·무선 네트워크 및 센싱 기술을 기반으로 환자, 병원, 정부기관 등이 유기적 연계를 통해 실시간으로 국민의 건강 상태를 체크하여 삶의 질을 향상시켜 줄 수 있는 수단으로 부각되고 있다.

이에, 본 논문에서는 u-Healthcare 서비스의 추진현황을 분석하고, 안전하고 신뢰성 있는 u-Healthcare 서비스를 제공하기 위한 첫번째 단계로u-Healthcare 서비스 제공 방식 및 서비스 구조에 따른 정보보호 위협을 분석하여 제시한다 이러한 위협 분석의 결과는 향후 u-Healthcare 서비스의 정보보호 체계 구축을 통한 서비스 안전성 확보에 활용될 수 있을 것이다

2. u-Healthcare 서비스 위협분석 방법론

본 논문에서는 u-Healthcare 서비스의 위협 분석을 위해 아래와 같은 신규IT서비스 위협분석 방법론을 적용하고자 한다.[1]



(그림1) 위협분석 절차도

첫번째 단계인 서비스 아키텍처 분석단계에서는 신규 IT서비스의 서비스 제공의 목적 대상, 기능을 분석하여 서비스 개념을 정의한다 또한 본 단계에서는 서비스의 주요 구성요소, 통신프로토콜 등 주요 요소기술을 도출한다.

두번째 단계인 보호대상 식별단계에서는 첫번째 단계에서 정의된 서비스 개념과 서비스 아키텍처를 기반으로, 신규 서비스에서 보호해야 될 주요 보호대상을 선정한다.

세번째 단계인 위협 및 취약성분석 단계에서는 각 보호대상별 발생 가능한 보안위협을 도출한다 이때, 기존 ISP망에서 발생하였던, 보안위협 보다는 융합서비스로 인해 발생하는 위협을 중점적으로 도출하도록 한다

3. [1단계] u-Healthcare 서비스 환경 분석

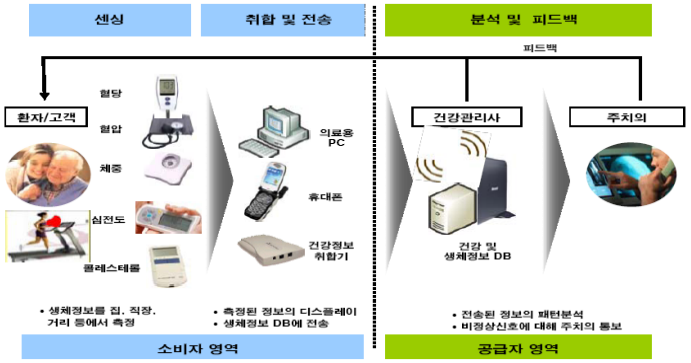
3.1 u-Healthcare 정의 및 흐름 분석

u-Healthcare는 ubiquitous computing과 healthcare의 결합으로 창출된 용어로, 현재 표준화된 정의가 되어 있

1) "본 연구는 TTA(Telecommunications Technology Association)의 [2010-P1-30] 차세대 바이오인식 응용기술 표준 사업의 일환으로 수행하였음."

지 않은 상태로, 유비쿼터스 환경을 이용하여 언제 어디서나, 건강상태의 평가, 진단 및 치료를 위한 모든 활동 제품 및 서비스를 제공하는 개념으로 보건의료와 IT를 연결 보건의료 서비스를 말한다[2][3]. 즉, u-Healthcare 서비스란 u-Health 환경을 통해 언제, 어디서나, 맞춤형 형태의 접근이 가능해진 소비자 중심적 보건의료 서비스이다. 여기에서 u-Health 환경이란, 보건의료체계에 ubiquitous computing이 도입됨으로써 보건의료자원과 서비스 전달체계의 지능화 및 네트워킹이 구현되어진 보건의료 환경을 의미한다.

u-Health의 구성과 흐름을 살펴보면 아래 그림과 같이 개인의 생체신호 및 의료정보의 측정 및 전송분석 및 피드백의 과정으로 분류되며 개인의 생체신호 및 의료정보를 측정해 의료기관 혹은 건강관리회사에서 운영하는 건강정보시스템으로 전송하면 시스템에서 전송된 정보의 패턴을 분석하고, 건강 관리사나 주치의는 대상 고객에 대해 원격으로 건강관리 및 의료서비스를 제공해 준다.



(그림2) u-Healthcare 서비스 흐름도

3.2 u-Healthcare 서비스의 특성분석

앞에서 살펴본 바에 따르면, 기존의 의료정보화와 비교하여 u-Healthcare의 기본속성은 의료기기에 내재화된 컴퓨팅에 의한 상황인식 기능 및 네트워킹 이를 통한 시공간적 접근성 증대, 궁극적으로 소비자 혹은 사용자 중심 패러다임으로의 변화의 반영으로 볼 수 있다. 의료기기의 지능화(intelligence)의 요소로는 상황인식(context awareness), 의사결정 지원 역량(decision support capabilities)을 들 수 있다.

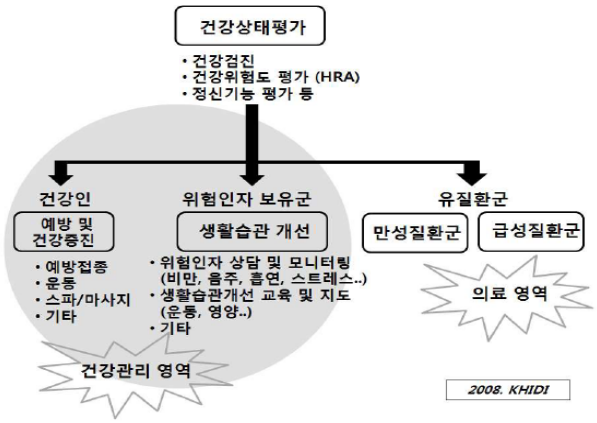
u-Healthcare 서비스는 보건의료서비스의 시간 및 공간영역의 확대가 가능하다. 특히, mobile device를 이용한 실시간 생체신호의 측정은 기존 의료서비스 공급 시간의 확대를 가능하게 하고, 화상 상담, 영상진료 등을 이용한 원격진료를 통해 대면진료로서만 가능했던 의료서비스의 공간적 제약을 해소할 수 있게 된다.

u-Healthcare 서비스의 또 하나의 특징은 개인 맞춤형 형태의 보건의료서비스의 제공일 들 수 있다. 지능화, 즉 특정 상황인식(context awareness)과 추론, 그리고 기타 보건의료자원과의 네트워킹이라는 ubiquitous computing의 속성은, 개인의 임상정보, 생체정보, 유전자 정보의 융합 및 광대한 용량의 보건의료정보DB의 패턴 마이닝 등을 통해 개인별 특성과 상황에 최적화된 임상의사 결정지원이라는 ubiquitous 산업이 지향하는 소비자 중심적인 서비스 접근을 가능하게 한다.

3.3 u-Healthcare 서비스 대상 및 영역분석

□ u-Healthcare 서비스 대상

기존 보건의료서비스 대상과 마찬가지로u-Healthcare 서비스의 대상도 의료서비스 대상자와 건강관리서비스 대상자로 분류하여 볼 수 있다[4][5][6].
현재 의료법은, 의료인의 자격 및 의료행위를 제한하고 있다. 또한, 환자를 대상으로 질환을 다루는 '의료서비스' 영역은 시설 및 인력 등 공급자적 측면에서 제한하고 있으나, 건강인 또는 위험인자 보유군(환자로 진단받지는 않았으나 건강에 위해적인 요소를 보유하는 자)을 대상으로 건강증진을 도모하기위한 서비스를 제공하는'건강관리서비스' 영역에 대한 공급 자격 등에 대한 제한을 위한 법적근거는 아직 마련되지 않고 있으나 최근 이를 제도 마련이 추진중이다. 즉, u-Healthcare라는 서비스의 대상은 대상자의 건강상태에 따라 의료서비스 대상자와 건강관리서비스 대상자로 분류될 수 있다[4].



(그림3) u-Healthcare에서의 의료와 건강관리 대상

□ u-Healthcare 서비스 영역

u-Healthcare서비스를 서비스 대상과 의료행위인 처치와 평가로 구분하여 분류하면 아래 그림과 같다[4].

(그림4) u-Healthcare 서비스 분류

첫번째로, "의료-평가" 영역은 u-모니터링(생체정보 파악, 운동량 파악, 위치파악 등), u-판독(방사선 영상, 병리화상 등), u-예측/맞춤의학(질병 발생 예측, 맞춤형 3D 가상 수술 등)이 속한다.

두번째로, "의료-처치"영역은 u-진료(상담, 처방, 지원, 자문 등), u-교육/지도(질환관리교육, 복약지도, 운동·영양지도, 원격재활교육 등), u-시술(원격수술, 케어로봇, 나노-바이오 수술로봇 등)이 속한다.

세번째로, "건강-평가" 영역은, u-생체/생활 정보 기반 건강평가 및 건강위험도 분석, u-바이오 정보 기반 건강위험도 예측 등이 속한다.

마지막으로 "건강-처치" 영역은 u-건강정보 제공,u-건강교육/지도 등이 속한다. 하지만, 실제로 u-Healthcare의 서비스에서는 각각의 분류영역에 두개 이상의 영역을 포함하는 서비스 모델이 등장할 것이다

4. [2단계] u-Healthcare 보호대상 식별

u-Healthcare 서비스 주요 보호대상으로는 앞의 서비스 흐름도에서도 제시하였던, u-Healthcare 의료기기, 게이트웨이, 통신프로토콜, 진단지원 시스템을 선정한다 각 보호대상의 구성과 역할을 좀 더 자세히 살펴보면 아래와 같다.

4.1 u-Healthcare 의료기기

정보통신기술을 이용하여 의료기관이 아닌 장소에서 일반인, 환자의 건강상태 체크와 건강관리 등의 의료서비스를 제공하기 위해 네트워크와 연계하여 사용되어지는 의료기기로, 센서부(생체신호를 감지하는 부분), 통신부(측정된 결과 값을 전송하는 통신 부분), 분석 및 표시부(측정결과에 대한 분석 및 표시하는 부분으로 통신망을 통해 별도의 장치(서버)에 분석결과를 표시해 주는 경우 분석 장치 포함)로 구성된다. u-Healthcara 의료기기는 사용자의 건강관리를 위한 체온 혈압, 혈당, 심전도, 심박수, 산소포화도 등 생체현상을 측정 및 관리하는 기능을 제공한다.

4.2 u-Healthcare 게이트웨이

사용자의 건강상태를 반영하는 주요 생체신호를 측정 센서로부터 수집한 후, 신호 자체 또는 신호 분석결과를 유/무선 통신망을 통해 u-Health 서비스센터에 있는 의료진에게 전송한 후, 의료진의 분석결과를 받아 사용자에게 제공해주는 장치로 통신모듈, 고속인터넷모듈, 화상통신모듈 등으로 구성되는 하드웨어와 의료정보를 수집 저장을 통해 안전한 웹사이트로 전송을 수행하는 응용프로그램으로 구성된다.

4.3 u-Healthcare 통신프로토콜

u-Health 의료기기로부터 획득된 정보를 u-Health 게이트웨이에 전송하거나 u-Health 의료기기의 사용에 필요한 정보를 u-Health 게이트웨이로부터 u-Health 의료기기로 전송하는데 사용되는 통신프로토콜로 블루투스, 지그비 등 근거리무선통신과 USB 등과 같은 유선통신이 적용된다.

4.4 u-Healthcare 진단지원 시스템

국민건강의 안전성을 보장하기 위한 관리객체로 u-Health 의료기기를 통해 얻어진 데이터를 기반으로 사용자의 건강평가 및 관리를 위하여 사용자와 의료인에게 정보를 제공하는 소프트웨어 u-Health 의료기기로부터 측정된 환자데이터를 활용하여 그 결과를 환자에게 제공하기 위한 시스템을 말한다

u-Healthcare 진단지원 시스템은, 의료기기에서 수집된 입력데이터 및 결과데이터 제공을 위한 사용자 인터페이스, 수집된 데이터를 분석 선별, 검사, 모니터링 하여 진단에 필요한 정보를 추측하기 위한 추론알고리즘 추론에 필요한 지식을 저장하기 위한 지식 베이스 등으로 구성된다.

5. [3단계] u-Healthcare 보안위협 및 보호대책(안)

u-Healthcare 서비스의 주요 보안위협은 다음과 같다

- o 화상시스템 해킹 : Cart Rack 장비의 취약점을 이용하여 화상시스템에 직접 침투 또는 화상 전송되는 데이터를 도청, 위변조 공격
- o 불법적인 접근 : 원격진료서비스, u-방문간호서비스, 재택건강관리서비스 등 u-Healthcare 서비스에 대하여 허가받지 않은 사용자가 불법적인 침투 공격
- o 무선 해킹 : 무선통신용 AP 또는 공유기의 무선망에 접근, 불법 침투
- o 도청/위변조 : 불법적인 접근 시도 후, 전송되는 데이터를 도청, 위변조
- o 의료장비 해킹 : 의료장비에 백도어 또는 원격터미널 클라이언트 등으로 권한을 획득
- o 웹 해킹 : 의료지원용 홈페이지 공격
- o 개인 및 의료정보 DB 해킹 : 웹과 연동되는 DB에 대하여 웹로직의 SQL Injection 취약점을 이용하여 DB에 접근 내부 중요정보를 획득
- o 의료망 침투 : 웹 모의해킹 후, 웹서버 권한을 획득 한 후, 연동된 내부망으로 2차적인 침투 시도

[표1] u-Healthcare 위협 및 보호대책

위협명	보호대책명
보건진료소 환자용 원격진료시스템에 불법적인 접근	①공유기 장비 계정에 강화된 패스워드 설정
	②PC장비 계정에 강화된 패스워드 설정
	③원격건강관리시스템에 방화벽 설정으로 외부 접근을 차단
	④PC 방화벽 설정
	⑤PC 자동업데이트 설정
	⑥PC 바이러스 백신 설정
	⑦원격 터미널 서비스 허용 설정 금지

보건진료소 환자용 원격진료 서비스 도청/위변조	①공유기 장비 계정에 강화된 패스워드 설정
	②PC장비 계정에 강화된 패스워드 설정
	③원격건강관리시스템에 방화벽 설정으로 외부 접근을 차단
	④네트워크 전송 패킷 암호화 적용
	⑤무선 네트워크 전송 패킷 암호화 설정
원격건강서비스 시스템 관련 네트워크 구간에 대량의 IP 패킷 발송	①인터넷 접속장비(공유기)의 방화벽 설정
	②공유기의 보안 기능 중 DoS 설정
원격건강모니터링 화상 시스템 영상디스플레이 장비를 이용한 공격	①외부의 침입이 발생하지 않도록 보안설정 강화(VOIP 보안 설정)
	②네트워크 전송 패킷 암호화 적용
의료기관(보건소, 의료원) 의사용 원격진료 시스템에 불법적인 접근 가능성	①PC장비 계정에 강화된 패스워드 설정
	②PC 방화벽 설정
	③PC 자동업데이트 설정
	④PC 바이러스 백신 설정
의료기관(보건소, 의료원) 의사용 원격진료 서비스 도청/위변조 가능성 점검	①공유기 장비 계정에 강화된 패스워드 설정
	②PC장비 계정에 강화된 패스워드 설정
	③원격건강관리시스템에 방화벽 설정으로 외부 접근을 차단
	④네트워크 전송 패킷 암호화 적용
	⑤무선 네트워크 전송 패킷 암호화 설정
의료기관(보건소, 의료원) 의사용 원격진료 서비스에 대량의 패킷공격으로 서비스 거부 가능성 점검	①인터넷 접속장비(공유기)의 방화벽 설정
	②공유기의 보안 기능 중 DoS 설정
댁내 재택건강관리시스템에 불법적인 접근 가능성	①PC장비 계정에 강화된 패스워드 설정
	②PC 방화벽 설정
	③PC 자동업데이트 설정
	④PC 바이러스 백신 설정
약국의 원격처방시스템에 불법적인 접근 가능성 점검	①PC장비 계정에 강화된 패스워드 설정
	②PC 방화벽 설정
	③PC 자동업데이트 설정
	④PC 바이러스 백신 설정
인터넷망을 통한 u-헬스케어지원센터 웹서버 취약점 공격	①웹어플리케이션 XSS(크로스사이트스크립팅) 취약점 제거
	②웹어플리케이션 SQL Injection(인젝션) 취약점 제거
	③웹어플리케이션 서비스상 불필요한 파일 및 디렉토리 제거
	④웹어플리케이션 에러페이지 조치
인터넷망을 통한 u-헬스케어지원센터 서비스에 대량의 패킷공격으로 서비스 거부 가능성 점검	①방화벽이나 웹어플리케이션에서 DoS 공격을 대비할 수 있는 보안 강화설정을 적용
	②백업이나 장애처리 시스템을 두어, 사고 발생에 효과적인 대응

6. 결론

현재 u-Health 서비스는 의료법에 저촉되지 않는 범위에서 네트워크를 통해 기본적인 건강 센싱 정보의 전달 등 소극적 서비스에 한정되어 추진되고 있으나 향후 보건복지부에서 의료 관련 법령 정비와EHR(Electronic Health Recording) 등 의료정보(개인 건강, 의료 관련 정보) 집적체계가 갖추어 지면 병원간 진료기록 공유 등 다양한 서비스가 가능해 지며, 이에 따라 정보보호에 대한 필요성 및 역할이 증대되리라 예상된다. 다른 정보화 분야에서와 마찬가지로 정보화 역기능을 제대로 예방, 대응하지 못할 경우 다른 분야보다 훨씬 큰 보안위협 가능성을 수반할 수 있다.

또한, 개인의료정보의 자기결정권 수준 정의, 처방전 유통 시 인증서를 이용한 암호화 요구사항, 의료정보DB의 접근 및 이용범위 제한 등 다양한 정보보호에 대한 이슈가 존재한다. 이러한 정보보호 이슈를 현 사업추진 초기단계에서 논의하여 u-Healthcare 서비스의 안정적인 보급과 활성화에 기여하여야 할 것이다.

Reference

[1] 신동훈, 김성훈, 이강신, " 신규 IT 서비스에 대한 정보보호사전평가 모델 연구", 한국정보처리학회 2005년 추계학술대회, 2005.11. pp.0991-0994
[2] 정우수, 지경용. 국내외 u-Health 산업동향 분석. 한국전자통신연구원 2007
[3] 김시연, 이윤태. u-Healthcare의 개념 및 보건의료 서비스에의 적용. 한국IT서비스학회. 2008
[4] 이윤태, 김시연, "u-Healthcare 활성화 중장기 종합계획 수립", 한국보건산업진흥원, 2008
[5] 의료법 제 2조, 제 5조, 제 27조: 2008
[6] 건강서비스 활성화 T/F: 보건복지가족부