스마트 헬스 케어의 보안 이슈 및 사례 연구

임권창* 정태을* 이창훈*
*서울과학기술대학교 컴퓨터공학과
e-mail:chlee@seoultech.ac.kr

The security issue and example experiment of smart healthcare

*Kwonchang Lim *Taeeul Jung *Changhoon Lee
*Dept of Computer Science, Seoul National University of Science & Technology

요 약

스마트폰과 소형 디바이스의 발달로 헬스 케어 시장은 큰 성장세를 보이고 있고 플랫폼을 제공하는 회사들 간의 치열한 경쟁이 시작되고 있다. 시장의 성장세와는 달리 데이터 보안에는 상대적으로 취약한 면을 보였다. 본 논문에서는 헬스 케어 보안이 허술한 사례들을 보이고 이에 대한 해결방안을 모색해 본다.

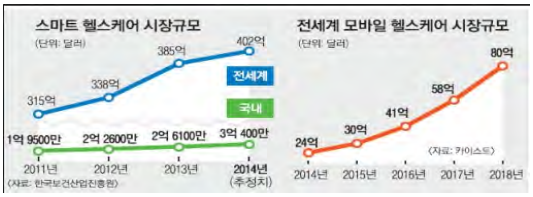
1. 서론

스마트 헬스 케어는 환자의 생체정보를 장소와 무관하게 수시로 수집한 뒤 외부의 의사가 분석을 해주는 서비스이다. 스마트 헬스 케어 분야는 센서 기술 개발에 주력하던 초기단계를 넘어서, 사용자 데이터 수집과 이를 이용하는 서비스 개발이 이뤄지는 단계로 진입하고 있으며, 헬스 케어 플랫폼을 제공하는 회사들 간의 경쟁이 시작되려 하고 있다. 하지만 자료 표준이 제정되어 있음에도 성장세에 밀려 지켜지지 않고 있는 실정이며, 아직도 표준 제정에 많은 기업들이 붙어있다. 표준이 지켜지지 않는 상황에서 보안적 허술함은 더 드러나고 있다. 본 논문에서는 스마트 헬스 케어의 현황과 전망, 그리고 보안 실태에 대해서 살펴보고 그에 따른 스마트 헬스 케어 보안에 대해서 분석한다.

2. 스마트 헬스 케어 동향

그림 1은 헬스케어 시장 규모를 보여준다. 국내외적으로 시장규모가 커지는 모습을 알 수 있다. 그리고 모바일 헬스케어 시장규모는 더욱 큰 기울기를 보이는데 이를 통해 IoT(Internet of Things)가 스마트 헬스 케어의 핵심 기술로서 사용자 데이터를 수시로 수집할 수 있는 기반이 되고 있다는 것을 알 수 있다.

<그림 1> 헬스케어 시장규모



최근 하드웨어 소형화에 따라 사용자 착용형 디바이스들이 등장하고 있다. 스마트폰과 연계해서 자동 진단 시스템이 가능해졌으며, 노령화 인구의 증가 추세에 따라 건강에 대한 관심이 높아지고 있어 관련 상품 및 서비스가 늘어나고 있다.

<그림 2> Nike사의 FuelBand

예를 들면, 그림 2는 Nike사의 FuelBand 제품으로서, 사용자의 운동정보를 기록하고 분석해주는 서비스를 제공한다. 그 외에도, Apple사와 삼성의 스마트 워치등의 제품을 비롯해 다양한 IoT 기반 헬스 케어 제품들이 출시되고 있는 상황이다.

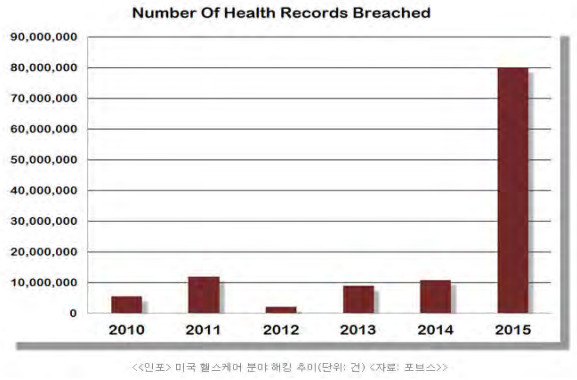
국외에서는 스마트폰과 모바일 어플리케이션, 전용 단말기를 위주로 헬스케어 시장이 성장하고 있으며. 국내에서는 통신사와 제조사가 보유한 기반을 이용해 사업 영역 확장 진행 및 기존 의료기관과 연계한 신규 사업을 추진중이다. 헬스 케어 산업이 커지는 것과 동시에, 의료시장의 개방 및 국제화에 따라 의료 정보의 교환 및 공유 문제가 이슈화 되고있다. 현재 헬스케어의 국제 표준이 존재

하긴 하나 아직도 표준을 위한 많은 연구가 진행중이다. 사물인터넷 관련 표준화 작업은 IPSO Alliance, OMA, oneM2M, Zigbee, IETF 등의 다양한 국제표준기구에서 동시다발적으로 진행되고 있다. 그렇기 때문에 현재로선 헬스 케어 디바이스에서 수집되는 정보들이 서로 호환이 안되는 문제가 발생하고 있다.

3. 스마트 헬스 케어 보안

현재 헬스케어 분야는 최근 들어 진료자 개인 정보, 진료 상태 등 데이터의 디지털화가 급속히 진행되면서 데이터 양도 크게 늘고 있지만 상대적으로 보안은 매우 허술한 상태로 진행되고 있다. 미국 정보보안 전문가들은 올해를 '헬스케어 분야 해킹의 해'로 경고했고 로이터와 포브스 등 주요 외신에 따르면 헬스케어 산업이 전세계 해커 세력의 새로운 공격 대상으로 떠오르고 있다.

<그림 3> 헬스케어 분야 해킹 추이



<<인포> 미국 헬스케어 분야 해킹 추이(단위: 건) <자료: 포브스>>

이미 올해 초 전미 2위 건강보험 업체인 앤섬이 8000만 명에 달하는 자사 개인고객정보를 해킹 당해 고객들의 이름과 생년월일, 사회보장번호, 집 주소, 이메일 주소 , 소득 관련 정보 등이 유출됐다. 지난해에는 의료서비스업체인 커뮤니티헬스시스템즈의 환자 450만 명의 개인정보가 털리는 사건도 있었다. 지난 10년간 사이버 보안 범죄의 주요 타겟이 금융과 유통 분야였으나 방어체계가 강화되자, 해커들이 새로운 대상을 찾은 것이 헬스케어 분야라는 전망이다.

이러한 해커들이 헬스케어로 타겟 대상을 돌리는 것은 두 가지 이유가 있다. 첫째는, 많은 병원들이 모든 데이터를 전산화하는 데 집중하고 있는 것이다. 대부분 이러한 데이터를 어떻게 빨리 접속하느냐에 관심을 두고, 보안은 그 다음 문제로 생각하고 있는 상태이다. 둘째는, 해커들은 병원 시스템에 저장된 나이, 성별, 이름, 사진 등의 빅데이터를 단순 의료정보라고 보지 않는다. 개인 식별정보부터 카드정보까지 한 번에 여러 정보를 얻을 수 있는 데이터 모음집으로 생각하기 때문에 그 가치가 큰 것이다.

현재 헬스 케어 사업은 모바일 기기를 결합한 제품이 많이 나오는 추세로 , 이젠 병원 내부뿐만 아니라 그 정보들이 외부로 확산된다. 이에 따라 헬스케어 보안은 더욱더 중요시 될 것으로 전망된다.

헬스 케어 보안 취약성

1) aiq 사의 smart shirt

<그림 4> aiq사의 Smart shirt

그림4는 AIQ사의 Smart shirt 이다. smart shirt는 EKG (심저도 검사),EEG(뇌파 검사), EMG(근전도 검사) 등을 통해 사용자의 데이터를 수집한다. 데이터 간의 통신은 bluetooth 방식을 이용하게 되며, 태양판을 이용하여 충전 방식을 제공한다. 또한, 카메라를 통한 시간 촬영도 가능하다.

이 Smart shirt는 다음과 같은 문제를 가지고 있다. 첫째로, 무선 네트워크 환경을 이용하기 때문에 보안 상에 취약하다. bluetooth를 이용했을 때 통신상에 보안 문제가 발생할뿐더러, 기본적으로 무선 네트워크 환경에 이용되는 암호 기술들은 상대적으로 경량화된 암호를 이용하기 때문에 상대적으로 덜 안정적이다. 둘째로, 그에 따라 저장된 데이터에 대한 개인 정보가 유출될 위험성이 있다. 마지막으로 AIQ 사의 제품은 데이터에 접근하고자 하는 사용자에 대한 인증 / 인가 기능을 지원하지 않기 때문에 보안상 취약하다.

2) BodyTel 사의 Gluco Tel, Pressure Tel, Weight Tel

<그림 5> BodyTel 사의 헬스케어 디바이스

그림5는 BodyTel사의 Gluco Tel, pressure Tel, Weight Tel로서 각각 사용자의 혈당, 혈압, 체중에 대한 데이터를 수집하는 역할을 한다. bluetooth를 통해 실시간으로 통신이 제공되며 스마트 폰, 온라인 웹 포털과의 연동 기능을 제공한다. 혈당과 혈압을 감지하는 주기는 각각 10초, 30초이다.

해당 제품도 다음과 같은 문제점이 있다. AIQ의 smart shirt와 마찬가지 bluetooth 사용으로 인한 통신 보안 문제와 데이터에 접근하고자 하는 사용자에 대한 인증/인가 기능이 지원되지 않아 누구나 열람 가능하다. 또한 센싱 데이터 저장 시 데이터에 대한 암호화가 되지 않는 문제가 있다. 마지막으로 웨어러블 기기의 센싱 주기 사이의 오류 데이터 전송 공격이 가능하다.

3)Medtronnic 사의 Portable glucose level monitoring

<그림 6>Medtronnic 사의 헬스케어 디바이스

그림6은 Medtronnic 사의 Portable glucose level monitoring이다. 이 제품은 체내 혈당 모니터링 기능을 제공한다. 환자의 복부에 부착하며 베터리 전원 사용 방식이다. 무선 통신을 통한 데이터 전송 방식을 이용하고, 도킹 스테이션을 통한 베터리 충전, 데이터 전송이 가능하다. 또한 미국 FDA에 이미 승인 완료된 상태이다.

보안상의 문제로는 혈당량 데이터 저장 시, 데이터 암호화가 지원되지 않고 또한 데이터에 접근하고자 하는 사용자에 대한 인증 / 인가 기능 지원하지 않아 누구나 데이터에 대해서 열람이 가능하다. 마지막으로 RF 통신 보안 문제로 자체 RF 통신 프로토콜 사용으로 인해 보안이 적절히 지원되지 않아 보안상 취약하다.

4. 결론

스마트 헬스 케어 국내외 많은 기업에서 투자하고 있는 전망있는 분야이다. 글로벌 경쟁에서 앞서가기 위해서는, 새로운 서비스와 고객들을 선점하는 것도 중요하지만 상대적으로 취약한 분야인 표준제정에 힘쓰는 것이 중요하다. 또한, 진료자의 의료 관련 자료들에 대한 디지털화의 속도에만 치중하는 것이 아닌 데이터 암호화의 큰 비중을 둬야한다.

현재 헬스 케어 분야의 공통적인 취약점은 무선 네트워크 보안에서 발견되고 있다. 이를 방지하기 위해선 우선적으로 무선 네트워크 상에서 오가는 데이터에 대한 암호화가 안전하게 이루어져야 한다. IOT 헬스 케어 분야에서 이용되는 대부분의 프로세서들은 상당히 낮은 비트로 구현된다. 그렇기 때문에 현재 경량화 암호의 대표적인 암호인 LEA, HIGHT, 타원 곡선 암호를 낮은 비트에서 구현할 수 있는 기술에 대한 연구가 선행되야 한다.

참고문헌

[1] 류경동 "헬스케어, 해커들의 새로운 먹잇감 표적" etnews.com
[2] 이지현 "2015년, 병원 해킹 사건 늘어날 것" bloter.net
[3] "사물인터넷 기반 헬스케어 서비스 및 플랫폼 동향" 경북대학교