원격의료 서비스의 개인정보 침해 시나리오 개발

최현욱*, 김택영**, 김태성***
*충북대학교 융합보안협동과정
**충북대학교 보안경제연구소
***충북대학교 경영정보학과
chwin304@naver.com, ecac987@naver.com, kimts@chungbuk.ac.kr

A Scenario Development on the Personal Information Breach in Telemedicine Service

Hyun-Wook Choi*, Taek-Young Kim**, Tae-Sung Kim***
*Dept. of Convergence Security, Chungbuk National University
**Cybersecurity Economics Research Institute, Chungbuk National University
***Dept. of Management Information System, Chungbuk National University

요 약

4차 산업혁명 시대가 도래함에 따라 사물인터넷(IoT)이 다양한 산업의 영역에서 활용되고 있다. 특히 IoT 기술 및 서비스를 활용하는 분야 중 하나인 스마트 의료 분야는 최근 소프트웨어 및 네트워크의 연결성이 강화되면서 사이버보안 사고가 급증하고 있다. 따라서 스마트 의료 기기·서비스 개발 단계부터 보안을 고려하여 안전하게 개발하는 것이 필요하며, 서비스 제공시에도 보안을 고려하여 안전하게 관리 및 서비스를 제공하는 것이 필요하다. 이에 본 연구에서는 IoT 서비스 활용 분야 중 스마트 의료 분야에서 원격의료 서비스의 개인정보 침해 요인을 도출하고 이를 토대로 어택트리 기반의 시나리오 분석을 수행하고자 한다.

1. 서론

4차 산업혁명 시대가 도래하면서 사물인터넷, 클라우드, 빅데이터, 모바일, AI의 중요성이 증가하고 있다. 특히 사물인터넷(Internet of Things, IoT)은 다양한 산업의 영역에서 활용되고 있으며, 어플리케이션, 네트워크, 센서, 미들웨어 등 여러 계층을 연결하는 핵심 기술로서 각 분야 데이터의 융합과 공유 기반을 마련하는데 큰 역할을 수행한다.

IoT 산업은 헬스케어/의료, 에너지/검침, 제조, 스마트홈, 교통, 물류 등 다양한 분야에서 활용되고 있다[1]. 또한, IoT 산업의 총 매출액(내수/수출)은 2019년 전년대비 16.2% 증가하여 10조 원을 돌파하였으며, 2020년 총 매출액은 약 13조 원으로 조사되었다[1][2]. 하지만 IoT 산업과 기술의 성장과 더불어 다양한 IoT 기반의 제품과 서비스들에 발생하는 보안 위협이 증가하고 있으며, 그로 인한 피해 역시 기업뿐만 아니라 사용자에 이르기까지 폭넓게 발생하고 있다.

스마트 의료 분야는 최근 네트워크 기반의 의료기기 및 의료정보시스템의 증가와 인공지능, 빅데이터 등 최첨단 기술이 빠른 속도로 의료기관 내외의 각종 관련 시스템에 도입됨에 따라, 환자정보를 포함한 민감한 개인정보가 수집·유통·활용되고 있다. 이에 따라 의료기관 및 정보를 대상으로 하는 사이버 공격의 위협이 급증하고 있다. 실제 2017년 5월에 발생한 워너크라이 랜섬웨어 공격으로 영국의 '국민건강서비스(NHS)' 산하 40여 개의 병원 PC가 감염되어 모든 의료 서비스가 중단된 사태는 의료기관의 정보보호 취약성과 위험성을 단적으로 보여주는 예라고 할 수 있다[3].

스마트 의료 및 디지털 헬스케어 기기·서비스 개발단계부터 보안을 고려하여 안전하게 개발하는 것이 필요하며, 서비스 제공시에도 보안을 고려하여 안전하게 관리 및 서비스를 제공할 수 있도록 하는 것이 필요하다[4].

IoT 서비스의 확대와 함께 보안 위협의 증대는 기존 보안 솔루션으로는 대응에 한계가 있으며, 기존의 보안 대책으로는 내부의 중요한 정보가 유출되는 등의 위협에 대해서 방지하기가 매우 어렵다[5].

또한 공격자의 공격으로 인해 차량, 홈·가전, 헬스케어 등 IoT 서비스를 구성하고 있는 디바이스 및 관련 시스템의 오작동이나 불법조작이 발생하게 되면, 이용자의 신체나 생명, 재산에까지 피해가 발

생할 수 있고, 피해 범위도 사회 전반에 파급이 가능하다[6].

본 연구에서는 IoT 서비스 활용 분야 중 스마트 의료 분야의 원격의료 서비스 개인정보 침해 요인을 도출하고 이를 토대로 어택트리 기반의 시나리오 개발을 수행하고자 한다.

2. 선행 연구

2-1. IoT 보안 위협

IoT의 보안 위협 분류를 위해 먼저 IoT의 계층을 분류하는 것이 필요하다. IoT는 Sensing Layer, Network Layer, Middleware Layer, Application Layer 총 4계층으로 분류할 수 있다[7].

Sensing 계층은 센서를 이용해 물리적 현상을 감지하거나, 엑추에이터를 통해 감지된 데이터를 기반으로 특정한 작업을 수행할 수 있는 계층이며, Sensing 계층의 주요 보안 위협으로는 노드 캡처, 부팅 공격 등이 있다[7].

Network 계층은 Sensing 계층에서 받은 데이터를 계산 장치로 전송하는 역할을 수행하며, 주요 보안 위협으로는 DDoS/DoS 공격, 피싱 공격, 라우팅 공격 등이 있다[7].

Middleware 계층은 Network 계층과 Application 계층 사이에 추상화 계층을 만드는 역할을 수행하고 컴퓨팅 및 스토리지 기능, API 기능 등을 제공한다. 이 계층에서의 주요 보안 과제는 DB 보안 및 클라우드 보안이며, 주요 보안 위협으로는 중간자 공격, SQL 인젝션 공격 등이 있다[7].

Application 계층은 사용자에게 서비스를 제공하는 계층이며, 데이터 탈취 및 개인정보보호 문제와 같은 특정 보안 문제가 존재한다. 이 계층에서의 주요 보안 위협은 데이터 탈취, 접근 제어 공격, 악성 코드 공격, 스니핑 공격 등이 있다[7].

2-2. 스마트 의료 보안 위협

미국의 개인정보 유출 사례 등을 조사, 연구하는 비영리기구인 신용도용범죄정보센터에서 2017년 1월 18일에 발표한 2016년 데이터 탈취 동향보고서에 따르면, Healthcare/Medical 분야에서 전체의 약 34.5%에 달하는 데이터 침해사고가 발생했고, 보건 의료정보 관련 데이터 도난과 유출 사고 건수는 2005년 이후 약 400% 가량 증가했다고 보고했다. 의료정보를 보호하기 위해 미국의 경우 1996년 HIPPA(The Health Insurance Portability and Accountability Act)를 제정하여 의료정보에 대한 접근권한이 있는 의료기관 및 보험회사들에게 법령을 적용하고 있다. FDA는 2013년 6월 FDA 사이버 보안지침을 발표하여, 의료기기와 관련된 사이버보안의 위험성을 확인하여 권한이 없는 무단 접근을 제한하고, 인증된 사용자들에게만 접근을 허용하는 절차를 마련하였다. 또한, 2017년 12월에는 취약점 모니터링 및 탐지, 환자에게 발생하는 위험/취약성 평가, 데이터 전송을 위한 암호화 적용 등을 지침에 추가하였다[8].

원격의료 정보보안 또는 원격의료 개인정보 침해에 관한 연구는 국내를 기준으로 바이오 인증을 사용한 원격의료시스템의 취약성 분석 및 대응방안[9], 클라우드 기반 원격진료 클러스터 구축 보안 모델 설계[10], 의료정보 유출의 문제점과 의료정보보호[11]와 같이 다양한 분야로 진행되었지만, 원격의료 개인정보 침해 시나리오에 관한 연구는 활발하게 진행되고 있지 않다.

2-3. 시나리오 기반 보안 위험 분석

시나리오 기반 리스크 분석을 통해 향후 발생할 수 있는 사고를 자세히 조사할 수 있다. 그러나 기존 시나리오 기반 보안 위험 분석은 아티팩트를 명시적으로 정의하지 않거나 표준 표기법이 없기 때문에 추상적이라는 한계점이 있다[12].

따라서 Kim and Cha(2012)는 Use case diagram과 UML (Unified Modeiling Language)을 활용하여 보안 위험을 관리할 수 있는 위협 시나리오 기반의 보안 위험 분석 방법론을 제안하였다[12]. 이를 검증하기 위해 광대역 통신망(Broadband convergence Network, BcN)의 보안 위협인 세션 메시지 수정(Modification of Session Message)에 대한 유스케이스 다이어그램과 유스케이스 기술서를 작성한 후, 시나리오를 도식화하였다. 제안된 방법을 활용하면 보안 위험의 관리를 책임지는 의사 결정자들에게 효과적인 지침을 제공할 수 있다고 밝혔다[12].

2-4. Attack Tree의 개념

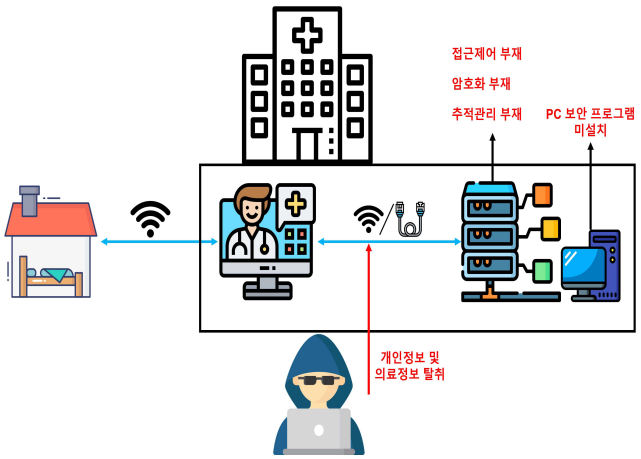
Attack Tree는 Schneier(1999)에 의해 처음으로 제안된 분석 기법이다[13]. 다양한 공격에 의거하여 시스템 보안의 특징을 규정짓는 체계적인 방법이며, 공격에 사용되는 모든 가능한 접근 수단을 검토할 수 있게 하여 대응책의 파악과 적용의 최적화를 용이하게 한다[14].

어택트리 구조는 루트 노드(Root Node)의 최종 공격 목적과 중간 노드(Sub Node)들의 목적을 달성하기 위한 다양한 공격 방법들을 묘사한다. 노드들은 일반적으로 선택 가능한 'OR' 노드와 목적을 달성하기 위해 반드시 수행해야 하는 'AND' 노드로 구성된다. 어택트리가 설계되면 여러 중간 노드들에게 가치를 할당하여 각각의 노드들의 가치를 계산하고 그 가치에 따라 보안 대책을 수립하게 된다[15].

3. 원격의료 개인정보 침해 시나리오

3-1. 침해 요인 식별 및 시나리오 도식화

본 연구에서는 원격의료 서비스의 시나리오를 도출하고, 시나리오 작성을 위한 구체적인 구성 요소들을 정의했다. 시나리오는 언론 보도[16]와 의료정책연구소의 보도 자료[17]를 참고하여 발생 가능한 위협, 위험 등을 반영하여 작성하였다. 정의한 구성요소들의 목록은 스마트 서비스, 용도, 구성 기기, 수집·활용된 개인정보 유형, 향후 문제 발생 요인, 주요 위협 및 취약점이다. 도식화한 시나리오는 <그림 1>과 같다.



<그림 1> 원격의료 서비스 개인정보 침해 시나리오 도식화

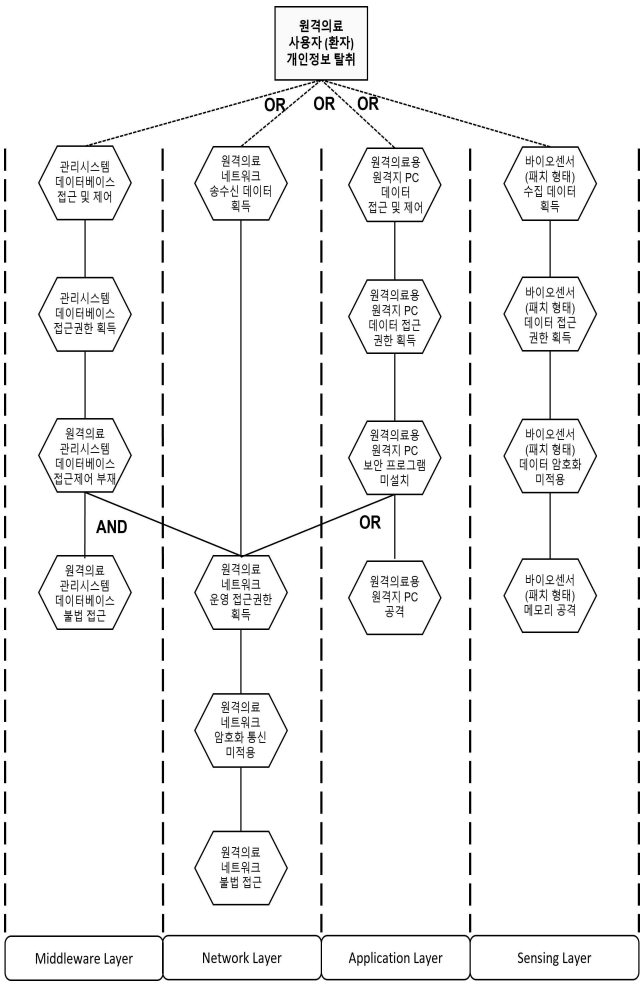
도식화한 시나리오의 구성 요소들의 정의는 <표 1>과 같다.

<표 1> 원격의료 서비스 개인정보 침해 시나리오 구성요소

구분	내용
스마트 서비스	스마트 의료
용도	소비자용
구성 기기	일반 기기, 센싱 및 엑츄에이팅 기기, 데이터 전송 기기
수집·활용 개인정보	일반정보(이름, 생년월일, 주소 등), 의료정보(의료기록, 질병내역, 약제 처방 내역 등)
향후 문제 발생 요인	공격자가 환자의 의료 정보, 개인정보를 대량으로 탈취하여 금전적 요구를 할 경우, 2차 피해가 발생할 수 있음
발생 가능 위협	① 네트워크 공격 ② 메모리 공격 ③ 시스템 공격
주요 취약점	시스템: 접근제어 및 추적관리 부재 네트워크: 비암호화 통신, 접근제어 부재 디바이스: PC 보안 솔루션 미설치

3-2. 어택트리 기반 개인정보 침해 시나리오

도식화한 시나리오와 정의 내린 구성요소를 기반으로 어택트리 분석 기법을 활용한 개인정보 침해 시나리오를 작성하였다. 최종적인 어택트리 기반 개인정보 침해 시나리오는 <그림 2>와 같다.



<그림 2> 어택트리 기반 원격의료 서비스 개인정보 침해 시나리오

4. 결론

본 연구에서는 원격의료 서비스에 대하여 상대적으로 미흡하였던 개인정보 침해와 관련된 분야에 대하여 제품 및 서비스의 설계 단계에서부터 위협에 대응할 수 있는 시나리오를 제안했다. 의료 분야의 IoT 활용은 국민들에게 제공되는 의료 서비스의 품질 향상과 더불어 의료 서비스 제공 범위의 확대를 도모할 수 있다. 하지만, 민감 정보에 해당하는 의료 정보가 네트워크를 통해 송·수신되기 때문에 높은 수준의 정보보안이 요구된다. 이에 따라 의료 분야의 IoT 보안 기능을 강화하고, 사용자의 프라이버시를 보호하기 위해서 제품 및 서비스 설계 단계에서부터 보안 위협을 구체적으로 정의하고, 예상 시나리오를 분석하여 잠재적인 위협에 대응할 수 있는 체계를 구축하는 것이 필요하다.

향후에는 의료 분야뿐만 아니라, IoT 환경에서 발생할 수 있는 개인정보 침해 시나리오 개발 및 개발 방법을 정립함으로써 발생할 것으로 예측되는 또는 예측 불가능한 사이버 위협에 선제적으로 대응할 수 있는 기반을 마련하고, 더 나아가 '인공지능 기술 기반 IoT 개인정보 침해 탐지'와 같은 보안 관련 신규 기술 개발에 활용이 가능할 것이라 기대한다.

참고문헌

[1] 과학기술정보통신부, 2020년 사물인터넷 산업 실태조사 보고서, 2021.

[2] 과학기술정보통신부, 2019년 사물인터넷 산업 실태조사 보고서, 2020.

[3] 한국인터넷진흥원, 스마트의료 사이버보안 가이드, 2018.

[4] 한국인터넷진흥원, 디지털헬스케어 보안모델(요약본), 2021.

[5] 김정녀, 진승헌, 초연결 환경에서 보안위협 대응을 위한 사물인터넷(IoT) 보안 기술 연구, 한국통신학회지(정보와통신), Vol. 34, No. 3, pp. 57-64, 2017.

[6] 행정안전부, 정부사물인터넷 도입 가이드라인, 2019.

[7] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B., A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, IEEE Access, Vol. 7, pp. 82721-82743, 2019.

[8] 김동원, 한근희, 스마트의료 환경에서 보안위협 대응을 위한 최근 연구동향, 한국통신학회지(정보와통신), Vol. 35, No. 2, pp. 95-99, 2018.

[9] 황유동, 이유리, 박동규, 신용녀, 바이오 인증을 사용한 원격의료시스템의 취약성 분석 및 대응방안, 한국통신학회논문지, Vol. 33, No. 2D, pp. 40-47, 2008.

[10] 안창호, 백현철, 박재홍, 김상복, 클라우드 기반의 전국 지방의료원 원격진료 클러스터 구축에 대비한 보안 모델 설계, 한국지식정보기술학회논문지, Vol. 11, No. 2, pp. 107-118, 2016.

[11] 전영주, 의료정보 유출의 문제점과 의료정보보호, 한국컴퓨터정보학회논문지, Vol. 17, No. 12, pp. 251-258, 2012.

[12] Y.-G. Kim and S. Cha, Threat Scenario-based Security Risk Analysis, Security and Commnunication Networks, Vol. 5, pp. 293-300, 2012.

[13] Schneier, B., Attack Trees, Dr. Dobb's Journal Vol 24, No. 12, pp. 21-29, 1999.

[14] 김경아, 이대성, 김귀남, 공격 트리를 이용한 산업 제어 시스템 보안 위험 분석, 융합보안논문지, Vol. 11, No. 6, pp. 53-58, 2011.

[15] 엄정호, 공격트리를 이용한 위협평가 방법에 관한 연구, 보안공학연구논문지, Vol. 9, No. 1, pp. 45-52, 2012.

[16] 연합뉴스, "의협 "원격의료 해킹에 무방비…공개검증 필요해"(종합)", http://www.yonhapnews.co.kr/bulletin/2015/02/25/0200000000AKR20150225065051017.HTML 2015.2.25.

[17] 의료정책연구소 보도자료, "보건복지부 2차 원격의료 시범사업 평가 결과에 대한 반박자료", https://rihp.re.kr/bbs/board.php?bo_table=report&wr_id=56&page=4, 2016.4.5.