Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.951

공격트리(Attack Tree)를 활용한 원격의료 보안위험 평가*

김 동 원,[1†] 한 근 희,[2] 전 인 석,[1] 최 진 영[2‡]
[1]고려대학교 정보보호대학원, [2]고려대학교 융합SW대학원

Telemedicine Security Risk Evaluation Using Attack Tree*

Dong-won Kim,[1†] Keun-hee Han,[2] In-seok Jeon,[1] Jin-yung Choi[2‡]
[1]Graduate School of Information Security, Korea University,
[2]Graduate School of Convergence Software, Korea University

요 약

현대의 의료분야는 스마트기기의 확산과 통신 기술의 발달로 스마트화 됨에 따른 의료보안 문제가 대두되고 있다. 그 중에서 원격의료는 의사-의사 간(D2D, Doctor to Doctor), 의사-환자 간(D2P, Doctor to Patient) 의료정보가 상호 교환되기 때문에 원격의료에서 발생할 수 있는 보안위험을 식별, 평가 및 통제하기 위한 위험관리 방안이 필요하다. 본 논문에서는 1차 의원, 보건소, 보건지소, 보건진료소 등에서 운용하고 있는 원격의료기기와 원격의료시스템을 현장에서 확인 한 결과를 토대로 공격트리(Attack tree) 방법론을 적용하여 원격의료에서 발생할 수 있는 보안위험 분석 및 평가 방법을 연구 제안한다.

ABSTRACT

The smart screening in the medical field as diffusion of smart devices and development of communication technologies is emerging some medical security concerns. Among of them its necessary to taking risk management measures to identify, evaluate and control of the security risks that can occur in Telemedicine because of the Medical information interchanges as Doctor to Doctor (D2D), Doctor to Patient (D2P). This research paper studies and suggests the risk analysis and evaluation methods of risk security that can occur in Telemedicine based on the verified results of Telemedicine system and equipment from the direct site which operating in primary clinics, public health centers and it's branches, etc.

Keywords: Telemedicine Security, Telemedicine Risk Management

I. 서 론

1.1 연구배경 및 목적

헬스케어 서비스는 과거의 일시적인 질환 치료에서 평생 개인 건강을 관리하기 위한 예방적 의료 서비스로 진화하고 있다. 이러한 헬스케어에 대한 인식의 변화와 함께 오늘날에는 다양한 스마트기기의 확산과 통신 기술의 발달로 스마트시대가 도래했다. 특히, 스마트 TV는 방송과 통신이 결합하고 융합하여 보다 다양한 콘텐츠를 제공하면서 헬스케어, 스마트 홈으로 서비스 영역을 확장시킬 수 있는 보다 능동적인

접수일(2015년 6월 22일), 수정일(2015년 7월 21일), 게재확정일(2015년 7월 21일)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1012)
† 주저자, blast.kim@gmail.com
‡ 교신저자, choi@formal.korea.ac.kr(Corresponding author)

매체로 발전했다. [1,2,5]. 이에 기존의 헬스케어 서비스는 병원 중심의 원격의료 단계에서 점차 홈 환경에서 이용할 수 있는 환자 중심의 smart-헬스케어 단계로 진화하고 있다. 개인 건강관리와 의료서비스를 보다 효율적이고 편리하게 제공받고자 하는 수요 증가와 함께 헬스케어 서비스를 통한 건강관리 서비스 기술 개발이 활발하게 진행되고 있다[3-5]. 의료기기의 해킹 가능성에 대한 연구의 예로 미국 오크리지 국립연구소 내 임베디드(내장형) 시스템 신뢰성센터의 나다니엘 폴 최고과학자는 2010년 동료 연구자와 함께 인슐린 펌프에 대한 해킹이 가능성 연구결과를 제시하였으며,[6] 2013년 7월 미국 라스베이거스에서 열린 블랙햇 2013 컨퍼런스에서는 의료사고의 이면을 여실히 보여주는 실험이 시연되었다. 이처럼 의료분야의 보안사고 발생가능성이 많은 연구를 통해 증명되고 있다.

1.2 연구방법 및 구성

본 연구에서는 원격의료 환경에서 보호해야할 자산에 대한 위협을 분석하고 평가함으로써 효율적인 보안대책마련을 위한 기반이 될 수 있도록 제안 하고자 한다. 본 논문의 II장에서는 의료분야 보안사고 사례 및 관련 연구에 대해서, III장에서는 원격의료 보안의 문제점에 대해 살펴보고, IV장에서는 연구대상인 원격의료 보안위험 분석을 위한 자산식별, 위협도출 및 평가를 연구하였으며, 마지막으로 V장에서는 본 논문의 결론으로 끝을 맺는다.

II. 관련 연구

2.1 원격의료 의의

원격의료 내지 원격진료(Telemedicine)는 상호작용하는 멀티미디어로써 음성, 동화상 등 각종 정보통신수단을 통하여 의료인이 환자를 직접 대면하지 않고서도 환자에 대한 진찰・검사・치료 등의 의료행위를 행하는 것으로 비대면진료의 성질을 지니면서 u-Health의 출현과 밀접한 연관을 지니고 있다. 원격의료의 유형으로는 ①대형병원 내의 PACS(Picture Archiving Communications System) 통신망을 이용하여 원격화상회의를 통해 환자의 치료에 대해 방향을 논의하는 원격자문, ②무선전화기・무선 통신 등을 이용한 화상 및 데이터 전송, 응급환자관리를 위한 치료지침을 제공하는 등의 원격의료, ③원격의료시스템을 활용하여 환자가 집안에서 의료기관의 진료를 받는 재택진료, ④의료인 및 환자에 대한 원격 교육, ⑤인터넷을 통한 의료상담 및 의료정보의 제공이 논의된다.[9]

2.2 의료보안 사고 사례

최근 우리는 크고 작은 의료정보 유출사고를 Table 1과 같이 경험했다. 실제 미국의 신용도용범죄정보센터(Identity Theft Resource Center)가 발표한 자료에 따르면, 지난 해 자체 수집한 약 9백만 개에 달하는 노출된 정보중 보건의료 관련 정보는 269건의 데이터 침해사고가 발생했다. 보건의료 관련 데이터 도난과 유출사고 건수는 2005년 이후 약 300% 가량 증가했다.[15] 또한 SANS는 2014년 2월 19일 의료산업에 대한 해킹위협 진단 연구보고서에서 의료정보 해킹에 대한 심각성을 제기하였다.[16] 첨단 ICT 기술과 의료가 결합된 원격의료(Telemedicine) 관련 정보는 개인신용은 물론 개인의 건강 및 민감정보를 담고있어 단순한 정보주체인 개인의 문제로 국한되는 것이 아니라 전 사회적인 위험이 될 수 있기 때문에 전 사회적 차원의 위험관리 방안이 모색되어야 할 것이다.

Table 1. Incidents and case in medical security

Year	Description	Ref
2009	For Medical Secrets, Try Facebook	[10]
2011	A Review of the Security of Insulin Pump Infusion Systems	[6]
2012	Hacker Shows Off Lethal Attack By controlling Wireless Medical Device	[11]
2013	Froedtert Hospital hacked, patients alerted of illegal access	[12]
2014	HealthSource of Ohio data leak exposed 8,800 patients information	[13]
2014	Hospital database hacked, patient info vulnerable	[14]

2.3 공격 트리(Attack Tree)

슈나이어(Schneier)에 의해 소개된 Attack Tree는 다양한 공격에 의거하여 시스템 보안의 특징을 규정짓는 체계적인 방법이며, 공격에 사용되는 모든 가능한 접근 수단을 검토할 수 있게 하여 대응책

의 파악과 적용의 최적화를 용이하게 한다. Attack Tree의 구성요소는 노드(node), 간선(edge), 커넥터(connector)이다. 각 노드는 공격을 나타내며 루트 노드(root node)는 공격자의 최종 목표이다. 개별공격 목표인 각 노드는 하위 공격 목표(또는 상위 목표를 달성하는 수단)인 자식 노드로 분해될 수 있다. 간선은 공격의 전이 상태를 표시한다. OR와 AND 커넥터는 2개 이상의 자식 노드들을 가진 노드의 공격목표 달성을 위한 전제조건으로 자식 노드들 중 1개만 선택 실행이 가능한 경우(OR)와 모든 자식 노드들이 반드시 실행되어야 하는 경우(AND)를 묘사 한다.[19] 본 논문에서는 원격의료에서 발생할 수 있는 보안위험을 공격트리(Attack tree) 방법론을 이용한 위험평가 방법을 연구 제안한다.

III. 원격의료 보안위협 분석

3.1 원격의료 보안위협 분석 방법

NIST는 각급 기관의 FISMA 구현을 위해 해당 표준과 지침을 전체적으로 통합하고 설명하기 위해 위험관리체계(RMF, Risk Management Framework)를 개발하고[21] 그 위험을 관리하기 위한 활동으로 위험이 기밀성, 무결성, 가용성 관점에서 정보와 시스템에 잠재적으로 미치는 영향도에 기반을 두어 분류(Categorize), 최소보안요구사항, 비용분석 등의 요소에 기반하여 최소 보안통제(Select) 선택, 보안환경에 맞게 실제 구현(Implement), 운영 등이 원하는 결과를 도출하였는지 평가(Access), 조직운영 및 자산 등 위험을 판단하고 받아들일 수 있는지 결정(Authorize), 보안 상황 모니터링(Monitoring)의 6단계로 Security Life Cycle로 분류하고 있다. FIPS PUB 199(Federal Information Processing Standards Publication 199)에서는 보안을 표현하기 위한 공통 Framework와 이해를 제공하기 위해 정보 및 정보시스템에 대한 보안 분류 기준(조직의 잠재적 영향을 기초로)을 정의하였고, 기밀성, 무결성, 가용성을 보안목적으로 구분하고, 보안목적에 대한 보안침해 발생 시 개인이나 조직에서 발생하는 잠재적인 영향도를 Low, Moderate, High 세 단계로 정의하고 있다.[17]

본 논문은 1차 의원, 보건소, 보건지소, 보건진료소 등에서 시범사업으로 운용하고 있는 원격의료기기와 원격의료시스템을 현장에서 직접 확인한 결과와 보안위협 발생가능 시나리오를 구성하여 도출 및 분석한다.

3.2 원격의료 자산가치 평가 기준

위험평가에서 위협을 분류하는 기준은 다음과 같이 보호대상인 자산(Asset)별로 Fig 1.과 같이 총 자산가치를 산정하여 사용한다.

평가등급 구분을 위한 방안은 Table 2. 과 같이 3점 분류 방식을 적용하여 각 영역별 점수를 결정한 후, 이를 합산하여 총 자산가치 점수를 산정하고, 산출된 총 자산가치 점수에 따라 평가 등급을 결정한다.

자산가치는 Table 3와 같이 기밀성, 무결성, 가용성, 자산기여도 등의 영역별로 영향 수준을 평가하고 이를 반영하여 총 자산가치를 계산하면 3 ~ 12의 점수를 얻게되며, 이 점수 수준에 따라 Fig 1의 산식으로 자산가치에 따른 중요도 평가등급 분류를 산정하면 1~5등급의 중요도 평가등급을 얻을 수 있다.

Table 4.은 이렇게 얻은 자산가치에 따른 중요도 분류를 정의한 것이다.

자산가치 평가는 국제표준인 ISO/IEC 27005[8]와 ISO 31000 RM을 준용하여 위험을 분석/평가하고, NIST 800-37 RMF, FIPS PUB 199, FMECA(Failure Mode, Effects, and Criticality Analysis)[18]에 기초한 기밀성, 무결성, 가용성의 요소를 이용한 위험평가 방법을 준용하여 연구한다.

$$AV(asset\,value)_a = \sum_{i=1}^{n} AV_i$$

AV_a: 자산 (a)에 대한 자산가치의 총합 (3 ~ 12)
i: 영향받는 영역 (1 ~ 3, 기밀성, 무결성, 가용성, 자산기여도)

Fig. 1. The total effect is calculated

Table 2. Asset value evaluation criteria

Division	Low	Moderate	High
Confidentiality	1	2	3
Integrity	1	2	3
Availability	1	2	3
Asset Contribution	1	2	3

3.3 원격의료 시스템의 구성요소

원격의료는 병원 방문이 힘든 사람들을 위하여 직접 방문하지 않고 의료서비스를 하기 위한 시스템이다. 초고령화 사회에서는 반드시 필요한 의료서비스라고 할 수 있을 것이다. 원격의료는 의사-의사 간(D2D, Doctor to Doctor), 의사-환자 간(D2P, Doctor to Patient) 원격에서 의료정보가 상호 교환되기 때문에 중요한 의료정보들은 컴퓨터의 데이터(Data)로서 Online상에서 수집, 이용·제공, 저장·관리, 파기 된다.

원격의료는 크게 사용자 영역(사용자 or 환자, 원격의료단말기), 게이트웨이(Gateway), 원격의료 서비스 제공자(Telemedicine System, Medical Team 등)로 구분할 수 있으며, 정보의 흐름에 따른 보안위협 시나리오를 예상하면 다음과 같다.

① 사용자 즉, 환자가 사용하게 될 센싱(측정)용 하드웨어 및 소프트웨어를 통한 악성코드 유입 및 환자의 민감한 정보유출 가능성이 존재하며, 센싱(측정)용 기기를 통한 주 서버로의 접근 가능성 존재
② 의료정보 전송 구간인 네트워크를 통한 정보유출 및 데이터 변조 가능성 존재
③ 센싱(측정)된 정보를 취합 및 의료인에게 전송하기 위한 PC, 스마트기기 및 게이트웨이의 알려진 취약점을 이용한 공격 가능성 존재
④ 공급자 영역인 주 서버 및 질병정보 데이터베이스(Repository)의 취약점을 이용한 공격 가능성 존재

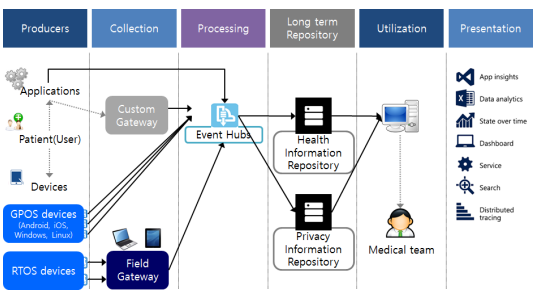

Fig. 2. Telemedicine system diagram

3.4 원격의료 위협도출 및 식별

원격의료의 공격트리(Attack Tree) 구성을 위한 위협을 식별하기 위해, ISO/IEC 27005를 참고하여 전형적인 보안위협, 인위적인 보안위협을 도출하고[8], ISO/IEC 27799 Annex A를 참고하여 의료분야 보안위협 도출[7]하여 재구성 하였으며, 또한, 원격의료 취약성을 식별하기 위하여, ISO/IEC 27005를 참고하여 원격의료에 맞추어 재구성하였다.[8] 이는 원격의료 공격트리(Attack Tree)를 구성하는 요소로서 활용된다.

식별된 보안위협과 취약성을 기본으로 원격의료 시스템 구성에 따라 원격의료 시스템의 보안위협은 Fig 3. Telemedicine security threat 7-point와 같이 7개 영역에서 발생할 것이다.

7가지 보안위협 시나리오는 다음과 같다.

① 환자 또는 사용자 : 현재 원격의료를 사용하는 환자 또는 사용자는 대부분 고령자이거나 IT 제품 사용에 익숙하지 않다. 또한 보안교육을 전혀 받아보지 않았거나 보안에 무관심하다. 이러한 환경에서 원격의료를 위한 단말기 사용에 따른 보안위협(기기조작 오류, 취약한 비밀번호 설정, 분실, 피싱 등) 발생가능성이 존재한다.
② 원격의료단말기 : 원격의료단말기는 크게 일반적기기(General System, GPOS)과 임베디드형 기기(Embedded System, RTOS) 2가지 형태로 분류할 수 있다. 임베디드형 기기는 제조사에서부터 기능에 최적화되어 생산되기 때문에 기기 내부로의 접근은 거의 불가능 하다고 할 수 있다. 다만 승인되지 않은 임베디드형 기기에 대한 통제방안은 필요할 것이다. 문제는 일반적기기 형태인 단말기로서 스마트폰, 스마트패드 등이 존재한다. 이러한 단말기는 OS 상에 별도로 개발된 응용프로그램이 동작하고, 무선네트워크

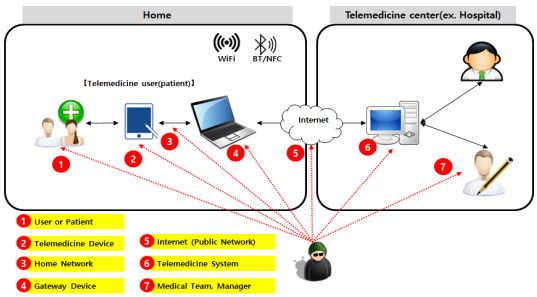

Fig. 3. Telemedicine security threat 7-point

(Wi-Fi, Bluetooth, NFC 등) 기능이 탑재되어있으므로, 이러한 환경에서 원격의료단말기 사용 시 다음과 같은 보안위협(단말기 내부 정보저장 및 유출, 단말기 분실/도난, 어플리케이션 취약점, 평문전송 등) 발생 가능성이 존재한다.

③ 홈 네트워크(Wi-Fi, Bluetooth, NFC, LAN, CDMA 등) : 원격의료단말기는 환자 개인의 공간 (Home, 사무실 등)에서 사용하는 경우 일부의 단말기는 무선네트워크를 이용하여 원격의료시스템(내부 시스템)과 정보를 송·수신 한다. Fig 4과 같이 홈 네트워크 상에서 사용하는 네트워크 기능은 로컬 유선 네트워크, WiFi, Bluetooth, NFC, 3G, 4G/LTE 등 다양하게 사용된다. 일부 임베디드형 단말기는 로컬 유선 네트워크로 한정되어 있지만, 일반형 기기인 스마트기기들은 다양한 경로를 이용해 원격의료시스템과 통신을 한다. 또한 중간에 노트북, 스마트패드와 같은 게이트웨이가 존재한다. 게이트웨이는 원격의료단말기와 원격의료시스템의 중간에 위치하면서 End-To-End 중계역할을 한다. 이러한 환경에서 홈 네트워크 사용 시 다음과 같은 보안위협(종단간 평문전송, MITM 공격 등) 발생가능성이 존재한다.

④ 게이트웨이(Gateway) 단말 : 게이트웨이는 원격의료단말기를 이용하여 환자 개인이 사용하여 정보를 전송하는 과정에서 원격의료시스템과의 중계역할을 한다. 환자 본인은 원격의료기기를 이용하여 측정한 정보(혈압, 혈당, 신체활동 등)를 Bluetooth, NFC, USB, WiFi, LAN 등을 이용하여 스마트폰, 스마트패드, 노트북 등과 같은 게이트웨이 단말로 데이터를 전송한다. 이러한 환경에서 다음과 같은 보안위협(Rogue 게이트웨이, 게이트웨어 분실/도난, MITM 공격 등) 발생가능성이 존재한다.

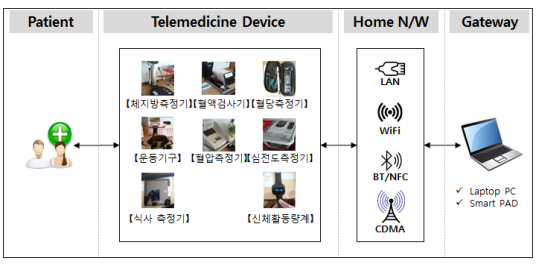

Fig. 4. Telemedicine Home Network

⑤ 인터넷 망 : 환자와 원격의료시스템과의 통신은 외부 인터넷망을 이용한다. 공개되어있는 네트워크를 사용하여 환자의 개인정보, 진료정보, 건강정보, 처방전 등을 송·수신하기 때문에 End-to-End 보안이 중요하며, 암호화 전송이 필수로 요구된다. 이러한 환경에서 원격의료시스템의 인터넷망 사용 시 다음과 같은 보안위협(스니핑, 위/변조, 권한상승 등) 발생가능성이 존재한다.

⑥ 원격의료시스템 : 원격의료시스템은 원격의료서비스 제공자 내부에 위치하고 있으며, 원격의료단말기와 통신하며 환자의 의료측정정보를 모니터링 하거나 진료목적으로 사용된다. 원격진료용 PC와 소프트웨어로 구성되며 의료진, 간호사, 시스템관리자(보안담당자, 관계자 등)가 사용하며 원격의료단말기를 사용하는 모든 환자들의 정보를 취급하므로 매우 중요한 시스템이라고 할 수 있다. 또한 원격의료시스템은 관계기관과 국가정보통신망을 이용하여 연결되어 있으므로, 본 시스템의 보안문제를 통해 국가 내부시스템으로의 침투가 가능하기 때문에 매우 높은 수준의 보안이 요구된다. 또한 특별한 경우, 예를 들면 원격진료소 등에서 운동기구와 원격진료용 컴퓨터 간 무선네트워크를 통해 통신을 하는 경우도 존재한다. 이러한 환경에서 원격의료시스템에서 다음과 같은 보안위협(MITM, 악성코드 감염, 원격진료용 어플리케이션 위변조, 물리적 통제 우회를 통한 국가정보통신망 접근 등) 발생가능성이 존재한다.

⑦ 의료진, 간호사, 시스템관리자(보안담당자, 관계자 등) : 원격의료시스템은 크게 의사-의사(D2D)간, 의사-환자(D2P)간 체계로 구분할 수 있다. 의사-의사간의 원격의료는 건강정보, 진료정보의 공유 및 모니터링 형태를 갖는다고 할 수 있다. 의사-환자의 원격의료는 실제 의사와 환자간 원격에서의 진료가 이루어지며 처방전까지 원격에서 발행하기 때문에 더욱더 높은 수준의 보안이 요구된다. Fig 5.는 의사-의사, 의사-환자 간의 원격의료 구성도이다. 이러한 환경에서 원격의료시

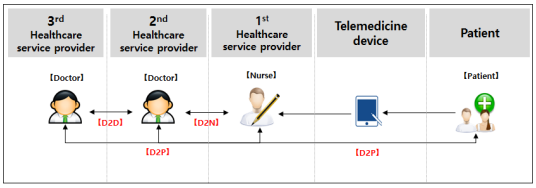

Fig. 5. Telemedicine medical team

스템에서 다음과 같은 보안위협(조작실수, 처방전 변조, 중요정보 유출, 도청 등) 발생가능성이 존재한다.

7-point에서 발생가능한 보안위협은 IV장 에서 공격트리(Attack tree) 구성을 통해 공격발생확률을 산정하기 위한 기반자료로서 활용된다.

IV. 원격의료 보안위험 평가

4.1 연구방법

슈나이어(Schneier)에 의해 소개된 공격트리(Attack Tree)는 다양한 공격에 의거하여 시스템 보안의 특징을 규정짓는 체계적인 방법이다.[19] Fig 6와 같이 공격트리(Attack Tree)의 공격을 나타내는 각 노드(node)의 공격목표 달성을 위한 전제조건 식인 OR, AND 커넥터를 통해 공격발생확률(Attack Occurrence Probability,이하 AOP)을 산정하기 위해 사용된다.

공격발생확률은 부모 노드의 공격목적을 달성하기 위해서 부모노드와 관련된 모든 공격노드 대비 자식노드의 공격 이벤트 발생비율을 의미한다. AOP는 다음과 같이 계산한다.[20]

Child node(이하 X)가 leaf node라면 $AOP=1$

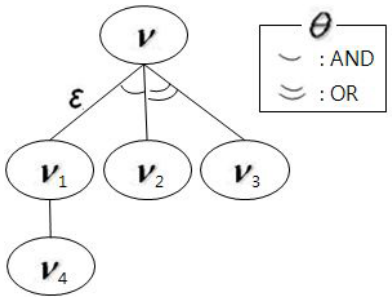

Fig. 6. Attack Tree

X가 AND조합이라면 $AOP=\frac{AND\text{조합수}}{X\text{수}}$

X가 OR조합이라면 $AOP=\frac{1}{X\text{수}}$

Fig. 7. The AOP is calculated

하지만 이러한 공격트리 시나리오에서는 각각의 노드의 가중치를 부여하지 않은 한계점이 존재한다. 각각의 노드마다 위협의 정도가 모두 동일하지 않으며, 그 위협으로 인한 피해정도 또한 다르다. 뿐만 아니라 각각의 노드 발생확률을 비교 한 것이 아니라, 하위 노드에서 상위 노드를 통한 공격 목적을 달성하기 위한 확률만 나타 낼 뿐, 각각 노드의 발생빈도와 위협의 정도를 고려하지 않았기에 단말기의 보안 위협의 정도를 수치화하여 표현하기에는 한계점이 존재한다.

4.2 원격의료 공격발생확률(AOP)

공격발생확률을 산정하기 위하여 원격의료 보안위협 7-point에 따른 각각의 보안위협 시나리오를 Fig 8의 예제와 같이 공격트리(Attack Tree)를 설계하여 공격발생확률을 산정한다.

Fig 8 예제의 공격발생확률을 산정하면, v_4의 단계로 넘어가는 방법은 v_8, v_9 두 개 중 한 개를 선택하는 방법이 있으므로 v_4는 $\frac{1}{2}$의 공격발생확률(AOP)을 가진다. v_2를 달성하기 위해서는 v_4, v_5,

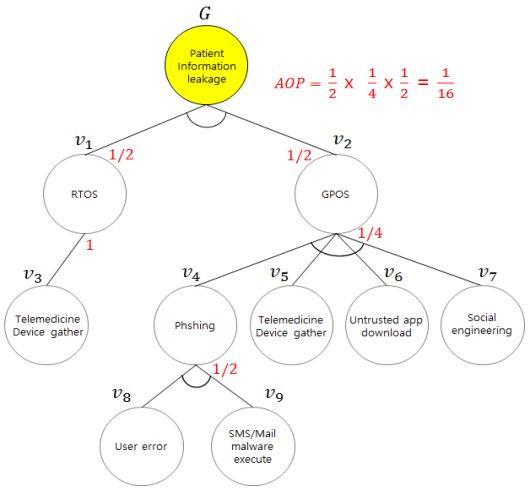

Fig. 8. User or Patient Attack Tree example

v_6, v_7의 4개의 방법 중 한 개의 방법을 선택하여야 하므로 $\frac{1}{4}$의 공격발생확률(AOP)을 가진다. v_1을 달성하기 위해서는 v_3 단일노드 방법을 선택하며 되므로, 1의 공격발생확률(AOP)을 가진다. 따라서 공격대상이 사용자 혹은 환자일 경우에 환자정보유출 공격발생확률(AOP)은 6.25% 이며, 산식은 다음과 같다.

$$\text{공격발생확률 } AOP = \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} = \frac{1}{16} \times 100$$

Fig. 9. The AOP is calculated example

Fig 3. Telemedicine security threat 7-point 와 같이 7개 영역에서의 공격트리를 설계하여 각각의 공격발생확률을 계산하여 평가등급 구분을 위하여 Table 5. 와 같이 3점 분류 방식을 적용하여 각 영역별 점수를 결정한다.

Table 5. Attack Occurrence Probability evaluation criteria

Division	Low	Moderate	High
	1	2	3
AOP	1~50%	51~80%	81~100%

4.3 원격의료 보안위험 평가 방법

원격의료 위험도(Risk value, 이하 RV)를 평가하기 위하여 "자산 중요도", "발생가능확률(AOP)"을 산정하고, 각각 특성에 따라 산정된 값을 서로 곱하여 위험등급을 평가한다.

$$Risk\ Value\,(RV) = Asset\ Value \times AOP$$

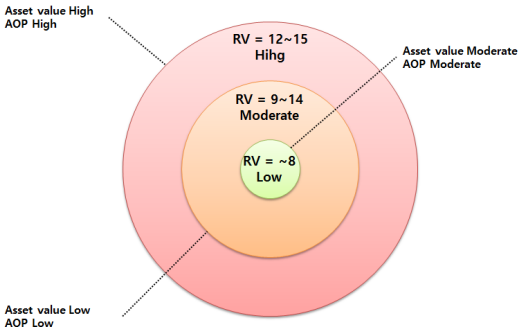

Fig. 10. risk evaluation criteria

산정된 위험도는 RV는 Fig 10와 같이 "높음(H)", "보통(M)", "낮음(L)"으로 분류하여 평가한다.

위와 같이 산정된 점수와 기준에 따라 자산별 "자산 중요도"와 보안위협에 따른 공격발생가능성을 계산한 위험평가 목록은 Table 6과 같다.

V. 결 론

원격의료는 본 논문에서 제시한 위험평가 방법을 통해 원격의료 보안위협 7-point 별 보안성을 유지하고 관리하기 위한 방법이 매우 필요한 실정이다. 이를위한 기반을 마련하기 위하여 본 논문에서는 원격의료 환경에서의 보안위협을 식별하고 평가하여 효과적인 보안대책을 마련하기 위한 방안으로서 도움이 될 것이라고 기대된다. 현재의 의료 환경은 ICT 외부인력에 의한 위탁관리 환경이 대부분이기 때문에 사이버 공격에 취약할 것으로 판단된다. 특히 의료보안 전문인력은 전무한 실정이며, 보안 위협 및 취약점 식별이 매우 필요한 실정이다. 본 연구는 원격의료를 활성화하고 보안성을 확보하기 위한 방안으로서 활용할 수 있다.

앞으로 나아갈 방향으로, 먼저 본 연구에서 제시한 원격의료의 위험평가를 토대로 실 환경에서의 모의검증을 통해 공격발생가능성을 검증하고 우선순위를 설정하여 효과적으로 보안위협에 대처할 프로세스 및 보안검증 방법에 대한 연구가 필요할 것이다.

Table 6 Definition of the Risk Value Evaluation List

Asset		Asset value	Concern	AOP	Risk assess	Risk value
Tele medicine Device	RTOS/ GPOS/ Gateway	5	Patient information leakage	1	5	L
		5	Weak password set	2	10	M
		5	critical information transmitted of device operation errors	3	15	H
		5	Loss due to improper management of Telemedicine device	2	10	M
		5	Access to internal system used of unapproved device	1	5	L
		5	Information leakage inside the device via malware infections	1	5	L
		5	Saving the important information inside the device	2	10	M
		5	Leakage of significant information by lost/stolen device	2	10	M
		5	Access to internal system and disclosure of important information by using application vulnerabilities of the device	2	10	M
		5	Device ↔ plaintext transmission between the internal systems	3	15	H
		5	Device ↔ plaintext transmission transmission between the Telemedicine System	3	15	H
		5	Device ↔ man-in-the-middle attacks between Telemedicine System	3	15	H
		5	Gateway ↔ plaintext transmission between internal system	3	15	H
		5	Information leakage by the malware infection (vaccine, latest patch, etc.)	1	5	L
		5	Significant information disclosure by gateway hacking	2	10	M
		5	Man-in-the-middle attacks by using rogue gateway	2	10	M
		5	Significant information leakage by lost/stolen gateway device	2	10	M
PC	PC	4	Forgery via wiretapping and spoofing	3	12	M
		4	Unauthorized access via man-in-the-middle attacks (MITM)	2	8	L
		4	Gateway ↔ plaintext transmission between Telemedicine System	3	12	M
		4	Man-in-the-middle attacks by using Rogue AP	2	8	L
		4	Information leakage by the malware infection (vaccine, latest patch, etc.)	1	4	L
		4	Significant information disclosure by gateway hacking	1	4	L
		4	Internal access to national communication networks via bypassing the physical security control	1	4	L
		4	Internal access to national communication networks via using wireless network vulnerability	1	4	L
		4	Leaving the working seat for long time after logging in	2	8	L
		4	Nonrepudiation failure by no saving the accessed record	1	4	L
		4	Accident due to telemedicine system operation errors	1	4	L
S/W	Telemedicine Software	4	Access to internal system and Important information disclosure via using application vulnerabilities of telemedicine treatment	1	4	L
		4	Access to internal system through the operation of application update files for telemedicine treatment	1	4	L
	Data transmit Software	3	Access to internal system and important information disclosure by using application vulnerability of data transmission	1	3	L
	Patient Medical Information Software	3	Access to internal system via operation of update files for software	2	6	L
	Monitoring Software	2	Access to internal system via operation of update files for software	2	4	L
	ECG Software	5	Access to internal system via operation of update files for telemedicine	2	10	M
Infor-mation	Personal Information	4	Sniffing	3	12	H
	Health Information	4	Health information sniffing	3	12	H
	Medical Information	5	Sending the invalid prescription through the medical info modulation during the telemedicine treatment	1	5	L
		5	Misuse of medical information through the opreation of network packet during the telemedicine treatment	2	10	M
		5	Accidents caused by telemedicine system operation errors	2	10	M
		5	Forgery via network eavesdropping and spoofing during the patient information exchange	2	10	M

References

[1] S. -H Kim, "Trend of personal health-device standardization for u-health service," Journal of KIISE Vol.29-1, pp.31-37, 2011.

[2] u-Health Forum Korea, 2009 u-Health Industry white paper, 2009.

[3] D.on-sik Yoo, "Review & Scheme of u-Health Standardization," TTA 20th Anniversary Seminar, Sep. 2008.

[4] Chan-young Park, "Technical trend of u-healthcare standardization," Electronics and Telecommunications Trends Vol. 25, pp. 48-59, Aug. 2010.

[5] Am-suk Oh, "A Study on Home Healthcare Convergence for IEEE 11073 Standard," JKIICE Vol.19 no. 2, pp. 422-427, Feb. 2015.

[6] N. Paul, "A Review of the Security of Insulin Pump Infusion Systems," Journal of Diabetes Science and Technology, 5(6), pp. 1557-62, Nov. 2011.

[7] ISO/DIS 27799:2014(E), "Health informatics - Information security management in health using ISO/IEC 27002," ISO, Feb. 2015.

[8] ISO/IEC 27005:2011, "Information security risk management (second edition)," ISO, Dec. 2011.

[9] Baek-Kyoung hee, "A Legal Study on the Relationship between In-Person and Remote Medical Treatments," Seoul Law Review, Vol. 21, pp. 449-482, Feb. 2014

[10] Katherine Chretien, "For Medical Secrets, Try Facebook," Journal of the American Medical Association, vol 302, pp. 1309, Sep, 2009

[11] Barnaby Jack, "Hacker Shows Off Lethal Attack By controlling Wireless Medical Device," RSA Conference, Feb. 2012

[12] http://fox6now.com/2013/02/14/froedtert-hospital-hacked-patients-alerted-of-illegal-access/, "Froedtert Hospital hacked, patients alerted of illegal access," fox6 now.com, Feb. 2013

[13] http://www.esecurityplanet.com/network-security/healthsource-of-ohio-data-breach-exposes-8800-patients-personal-info.html, "HealthSource of Ohio data leak exposed 8,800 patients information," eSecurity Planet, Mar. 2014

[14] http://www.wired.com/2014/06/hospital-networks-leaking-data/, "Hospital database hacked, patient info vulnerable," WIRED, Mar. 2014.

[15] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html, "Breach List Tops 600 in 2013," ITRC, Feb. 2015.

[16] SANS, "Widespread Compromises Detected, Compliance Nightmare on Horizon," SANS Health Care Cyber Threat Report, Feb. 2014

[17] NIST, "Guide for Mapping Types of Information and Information Systems to Security Categories," NIST SP800-60 vol. 1, Ayg. 2008.

[18] FMECA "Failure mode, effects and criticality analysis," FMECA MIL-P-1629, Jan. 2007.

[19] B. Schneier, "Attack Trees," Dr. Dobb's Journal, 24(12), pp. 21-29, Oct. 1999.

[20] Indrajit Ray and Nayot Poolsapassit, "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders," 10th European Symposium on Research in Computer Security, LNCS 3679, pp. 231-246, Sep. 2005.

[21] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems," NIST SP800-37 Rev. 1, Feb. 2010.

〈저 자 소 개〉

김 동 원 (Dong-Won Kim) 종신회원
2009년 2월: 서울과학기술대학교 컴퓨터공학과 졸업
2012년 2월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 2월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2014년 2월: 현대오토에버 정보보안기술팀 과장
2014년 3월~현재: 서울호서전문학교 사이버해킹보안과 전임교수
〈관심분야〉 시큐어코딩, 정보보호, 모바일 보안, 지능형 차량 보안, SSCA, 정형기법 등

한 근 희 (Keun-Hee Han) 종신회원
서울과학기술대학교 컴퓨터공학과 졸업
한양대학교 공학대학원 공학석사
고려대학교 대학원 이학박사
현재: 고려대학교 융합소프트웨어전문대학원 산학교수
〈관심분야〉 소프트웨어 보증, 시큐어 코딩, 정보보호관리 체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트 의료 보안, 스마트 자동차 보안 등

전 인 석 (In-seok Jeon) 종신회원
2009년 8월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 9월: 고려대학교 정보보호대학원 정보보호학과 박사 과정
2009년 9월~현재: Ahnlab CERT팀 주임 연구원
〈관심분야〉 네트워크보안, 정보보호관리체계, 정형기법 등

최 진 영 (Jin-Young Choi) 종신회원
1982년 서울대학교 컴퓨터공학과 (학사)
1986년 미국 Drexel University, Dept. of Mathematics and Computer Science (석사)
1993년 미국 Univ. of Pennsylvania, Dept. of Computer and Information Science (박사)
1996년~현재 고려대학교 컴퓨터-전파통신공학부 교수
〈관심분야〉정형기법, 임베디드 실시간시스템, 프로그래밍언어, 프로세스 대수, 소프트웨어 공학