https://doi.org/10.33778/kcsa.2021.21.1.063

보안성을 고려한 스마트 의료기기 관리(Secure-MEMP) 방법에 관한 연구★

김 동 원*

요 약

병원의 Biomedical engineering team은 의료기기가 안전하고 신뢰할 수 있도록 의료기기 관리 프로그램(MEMP, Medical Equipment Management Program)을 수립하고 규제할 책임이 있다. 기술의 발전으로 인공지능, 정밀의료 등 의료기기는 언제 어디서나 사물들 간 연결이 가능한 형태로 발전하고 있으며 다양한 기술의 융합에 따라 내외·부 보안위협이 지속적으로 증가하고 있다. 본 논문에서는 기술의 발전으로 지속적으로 증가하는 의료기기의 보안위협을 고려하여 안전한 의료기기 관리 프로그램(Secure-MEMP) 방법을 연구 제시한다.

A Study on the Smart Medical Equipment Management Program (Secure-MEMP) Method Considering Security

Dong-Won Kim*

ABSTRACT

The hospital biomedical engineering team is responsible for establishing and regulating the Medical Device Management Program (MEMP) to ensure that medical devices are safe and reliable. As technology advances, medical devices such as a rtificial intelligence and precision medicine are developing into a form that allows connection between objects anytime, any where, and as various technologies converge, internal and external security threats continue to increase. In this paper, we present a study of the Medical Device Management Program (Secure-MEMP) method, considering that the security threat of medical devices continues to increase due to advances in technology.

Key words : Healthcare security, Information security, Medical Equipment Management Program

접수일(2021년 2월 9일), 게재확정일(2021년 3월 18일)

★ 이 논문은 2020학년도 하반기 건양대학교 학술연구비 지원에 의하여 이루어진 것임.

* 건양대학교/사이버보안공학과

1. 서 론

1.1 연구 배경

최근 사물인터넷(IoT, Internet of Things) 기술의 발전으로 인하여 언제 어디서나 사물들 간 연결이 가능한 시대가 의료 • 전자 분야를 중심으로 추진되고 있다[1,2]. 헬스케어 서비스 는 향후 질병의 치료보다는 예방과 관리를 중요시하며, 진단, 수술 및 치료에도 확대 적용 가능한 서비스이다[3]. 헬스케어 분야는 사람들 사이에서 'Next Big Thing' 으로 불리며 많은 기대를 받고 있다[4,5,6]. 또한 Implantable Medical Devices (IMDs)는 신체 내에 이식되는 전자적 의료기기이며, 환자의 건강상태 모니터링, 신체 부위 기능 개선, 치료 등의 목적으로 사용된다[7]. 현재 IMD의 예로는 심장 상태를 모니터링하고 치료하는 심박조작기와 제세동기, 간질이나 파킨슨과 같은 경우 뇌심부 자극기, 주입 펌프 형태의 약물 전달 시스템, 그리고 다양한 생체 신호를 획득하고 처리하기 위한 다양한 생체 감지기가 사용되고 있다[8]. 특히 고급컴퓨팅 및 통신 기능을 보유한 IMDs는 환자에게 많은 이점이 있지만 수많은 보안 및 개인정보보호 위협이 존재한다. 특정 경우에는 치명적인 결과를 초래할 수 있다. 고의적인 오작동을 유발하는 경우 죽음을 초래할 수 있고, 미국 식품의약국(FDA)에서 인정한 바와 같이, 고의적인 공격은 우발적인 공격보다 훨씬 더 탐지하기 어려울 수 있다[9]. 또한 이러한 장치는 유럽(예: 지침 95/46/ECC) 및 미국(예: CFR 164.312) 지침에 따라 보호가 필요한 매우 민감한 의료 정보를 저장하고 전송한다[10][11]. IMDs에 대한 몇 가지 공격 중 무선 연결이 가능한 경우 치료기능을 비활성화하거나 재 프로그래밍(re-Programming)하고 환자에게 충격 상태를 유도하는 방법이 실험을 통해 입증되었다[12][13][14]. 또한, 배터리를 고의적으로 방전되도록 하여 장치가 작동하지 않도록 하였다. 이러한 경우에는 수술을 통해 IMD를 교체해야 하는 경우가 많다. 심장 IMD의 경우에는 자기장을 활용하여 쉽게 전원을 끌 수 있다[15]. 딕 체니 전 미국 부통령의 경우에는 이러한 우려로 Wi-Fi 기능이 없는 자신의 ICD(Implantable Cardioverter Defibrillator)를 다른 것으로 교체했다[16].

이처럼 의료기기는 환자에 대한 생명과 밀접하게 연결될 수 있기 때문에 보안관리의 중요성이 지속적으로 증가하고 있다. 특히, 기존 유선에서 무선통신으로 전송되는 대량의 데이터 처리 및 관리에 관한 보안 요구사항이 필수적으로 동반되고 있으며, 의료기기 개발에 있어서도 사이버보안의 중요성이 점차적으로 증가하고 있다[17]. 최근 발전하고 있는 다양한 의료기기들은 기능적으로 많은 발전이 이루어졌으나 이로 인하여 의료기기에서 발생할 수 있는 잠재적인 보안 위협도 함께 증가하고 있다. 의료기기의 해킹 가능성은 이미 많은 연구 보고가 되고 있으며[18][19][29], 의료분야의 보안사고 발생가능성이 많은 연구를 통해 증명되고 있다.

의료기기 또는 의료장비는 의료분야에서 중요한 역할을 하지만, 적절하게 사용되거나 유지 및 관리되지 않을 경우 해를 끼칠 수도 있다. 본 논문에서는 의료기기 유형별 보안위험 분석 및 연구를 통하여 의료기기를 안전하게 관리하기 위한 보안성을 고려한 의료기기 관리 프로그램(Secure - Medical Equipment Management Program) 방안을 연구하고자 한다.

1.2 연구방법 및 구성

본 연구에서는 스마트의료 환경에서 보안성을 고려한 안전한 의료기기 관리방법(Secure-MEMP)을 연구한다. 본 논문의 II장 관련연구 에서는 연구대상인 의료기기 관리 프로그램(MEMP)과 국내·외 의료기기 보안 현황 연구와, III장에서는 의료기기의 분류방법과 기능분석을 통한 의료기기 분류체계를 연구하였으며, IV장에서는 Use case 분석을 통한 의료기기 분류 별 보안위협 분석, V장에서는 활용방안, 마지막으로 VI장에서는 본 논문의 결론으로 끝을 맺는다.

2. 관련 연구

2.1 의료기기 관리 프로그램(MEMP)

병원의 임상 엔지니어링 부서는 의료 기기가 안전

하고 신뢰할 수 있도록 의료 장비 관리 프로그램을 수립 및 규제할 책임이 있다[20]. 기능 장애를 완화하려면 중요한 의료기기를 식별하고 우선 순위를 정해야 한다[20]. 의료기기의 종류 및 복잡성이 날로 증가함에 따라 병원은 중요한 기기가 안전하고 신뢰할 수 있으며 요구되는 성능 수준에서 작동하도록 의료 장비 관리 프로그램(MEMP, Medical Equipment Management Program)을 수립하고 규제해야 한다[20].

또한, 의료기기는 기술의 발전으로 언제 어디서나 사물들 간 연결이 가능한 형태로 발전하고 있으며 다양한 기술의 융합에 따라 내외·부 보안위협이 지속적으로 증가하고 있다.

Fennigkoh와 Smith(1989)는 의료기기의 Equipment Management (EM) 번호 또는 기기의 중요한 기능, 물리적 위험 및 필요한 유지보수에 할당된 수의 합계에 기초하여 의료기기를 그룹화하는 위험 평가 방법을 제안했다[20][21].(see Equation 1)

$$M \quad Critical\,Function + Physical\,Risk + Required\,Maintenance \tag{1}$$

1989년, 의료기관 인증위원회(Joint Commission on Accreditation of Healthcare Organization)는 이 방법의 중요성을 인정하였고(Fennigkoh and Smith, 1989) 결국 2004년에 표준(EC6.10)으로 승인하였다[20]. 기술의 발전으로 의료기기는 ICT 와 융·복합되고 있으며, 환자에 대한 생명과 밀접하게 연결될 수 있기 때문에 보안관리의 중요성이 지속적으로 증가하고 있고, 무선통신으로 전송되는 대량의 데이터 처리 및 관리에 관한 보안 요구사항이 필수적으로 동반되고 있으므로, 기존 Fennigkoh와 Smith model로는 사이버보안 위험에 따른 보안관리가 불가능한 실정이다. 이에 따라 본 논문에서는 의료기기 위협 분석을 통해 보안성을 고려한 Fennigkoh와 Smith model을 연구 제안한다.

2.2 의료보안 보안 요구사항

다양한 의료기기 및 의료장비를 사용함에 있어 예상하지 못한 위험으로 인하여 안전과 관련된 위협이 지속적으로 발생하여, 사람에게 물리적인 상해, 손상 또는 재산상의 피해를 초래하고 있다. 이러한 피해를 예방 또는 경감하기 위하여 위험관리(Risk management) 활동이 필요하며, 그 중요성이 지속적으로 증가하고 있다. 위험관리 제 품의 전 주기 동안 발생할 수 있는 모든 위험을 분석 및 평가하고, 이를 허용 가능한 수준으로 관리하는 시스템 또는 이러한 활동을 의미한다. 다양한 산업분야에서 위험관리가 필요하지만, 특히 환자는 대상으로 사용하여 안전성이 강조되는 의료기기의 경우에는 위험관리 활동을 수행하는 것이 더욱 중요하다. Table 1은 주요 국가별 의료기기 보안 현황이다[22].

〈Table 1〉 주요 국가별 의료기기 보안 현황

구분		주요내용
미국	FDA	• 의료기기 사이버 보안 관리지침 공개 • 무선 주파수 의료기기, 산업 및 식약청 직원을 위한 지침 공개 • FDA Safety Communication 운용: 의료기기 및 병원 네트워크에 대한 사이버보안 등의 권고사항 제시 • FDA 시스템 품질 규정 제시
	GAO	• 의료기기의 정보보안 대책에 대한 FDA 권고
	HIMSS	• Manufacture Disclosure Statement for Medical Device Security 공개
	DHS	• ICS-CERT Alerts 운용 : ICS-Alert-13-164-01 발표
	HITRIST	• CyberRX운용 : 의료기기에 대한 모의침투 공격 시행
	HIPPA	• Health Insurance Portability and Accountability Act 제정 및 공표
유럽	EU	• EC, EPHA, EMA의 기관을 운용하며 EU 관리 하에 3개의 의료기기 지침 발표 • 의료기기 지침, 능동형 이식 의료기기 지침, 체외 진단용 의료기기 지침 • 유럽 개인정보보호 규정(GDPR) 시행
일본	JIRA	• 제조업자에 의한 의료정보보안 개시 설명서 공개 • 원격 서비스 보안 가이드라인 공개
	JEITA	• 의료기기의 개발 및 보급 촉진 정책, 기술과제 대응 등의 활동
한국	KISA	• 스마트의료 사이버보안 가이드 공개
	KHIDI	• 의료기관을 위한 정보보호안내서 공개

의료기기 보안의 중요성은 지속적으로 증가하고 있으며, 이를 보호하기 위한 대책은 국제적으로 활발하

게 연구되고 있으며 표준화로 채택되고 있다. Table 2는 의료기기 보안관련 국제표준화 현황이다[22].

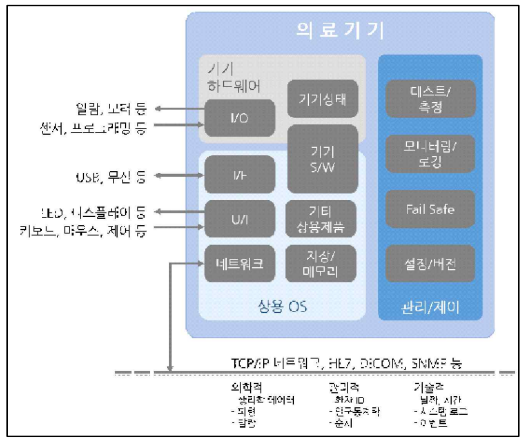
〈Table 2〉 의료기기 보안 국제표준화 현황

Standard	주요내용
IEC 62304	Medical Device Software – Software Life Cycle Processes
IEC 80001-1	Application of risk management for IT-networks incorporating Medical Devices
ISO 14971	Application of risk management to medical devices
ISO 13485	Medical devices -- Quality management systems -- Requirements for regulatory purposes
ISO 60601-1	Medical electrical equipment – Part 1: General requirements for basic safety and essential performance
ISO 60601-1-X	Medical electrical equipment – General requirements for basic safety and essential performance – Collateral Standard
ISO 60601-2-x	Medical electrical equipment – Particular requirements forthe basic safety and essential performance standards
IEC 62366	Medical devices – Application of usability engineering to medical devices
IEC 82304-1	Health software -- Part 1: General requirements for product safety
ISO/DTS ISO 11633-1	Health Informatics, Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis
ISO/TR 11633-2	Health informatics -- Information security management for remote maintenance of medical devices and medical information systems – Part 2: Implementation of an information security management system (ISMS)
ISO/AWI TR 22696	Guidance for an identification and authentication framework of networked Personal Health Devices(PHDs)
ISO 27799	Information security management in health using ISO/IEC 27002
ISO 10993-x	Biological evaluation of medical devices standards
UL 2900-2-1	Standard for Software Cybersecurity for Network-Connectable Products

3. 의료기기 분류체계

3.1 의료기기 분류

의료기기는 용도의 특수성과 규모, 복잡성 등으로 인해 하나의 통합된 아키텍처를 제시하기 어려울 정도로 다종다양하다. IHE (Integrating the Healthcare Enterprise)는 사이버 보안의 위협과 대응방법을 도출하기 위하여 이와 같이 다종다양한 의료기기의 특성을 통합하여 상위 수준의 중요 구성요소를 도출하여 일반적인 의료기기의 아키텍처를 다음 그림과 같이 제시하였다[30].



(Fig. 1) 일반적인 의료기기 아키텍처[30]

의료기기란 사람이나 동물에게 단독 또는 조합하여 사용되는 기구, 기계, 장치, 재료 또는 이와 유사한 제품으로서 ①질병을 진단, 치료 경감 또는 예방할 목적으로 사용되는 제품, ②상해 또는 장애를 진단, 치료, 경감 또는 보정할 목적으로 사용되는 제품, ③구조 또는 기능을 검사, 대체 또는 변형할 목적으로 사용되는 제품, ④임신을 조절할 목적으로 사용되는 제품 중 어는 하나에 해당하는 제품을 말한다[23]. FDA(Food and Drug Administration)는 의료기기에 소프트웨어의 비중이 높아짐에 따라 software as a medical device (SaMD)로 전환될 것으로 전망하고 있다[24]. 이에 따라 의료기기에 내장되어 있는 진료 및 의료 목적에 필요한 소프트웨어의 안전성 및 보안성 검증 방안이 매우 필요한 실정이다[25].

의료기기법 기준에 따르면 의료기관에서 일회용으로 사용되는 재료나 기구들도 의료기기에 포함되어 의료기기 보안관점에서 다루어져야 할 의료기기만을 분류하기에는 한계가 있다.

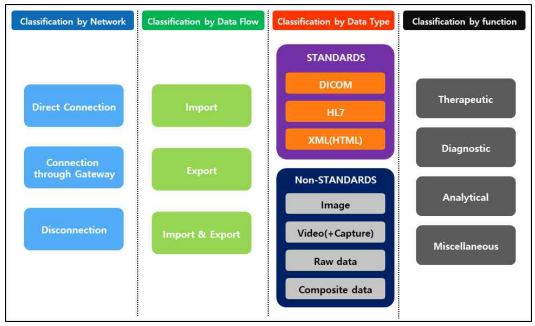
〈Table 2〉 고유기능과 사용목적에 따른 의료기기 분류체계

Standard	고유기능	대표 의료기기
LS (Life Support)	생명유지 기기	인공호흡기, CRRT, 심장충격기, 인슐린펌프, Pacemaker, 마취기, 신생아 보육기, 체외순환기 등
SR (SuRgical)	수술기기	수술내시경, Navigation, 로봇수술기, 전기(레이저)수술기 등
TR (TReatment)	치료 및 처치용 기기 (Physical Therapy and Treatment)	Gamma Knife, 선형가속기, 쇄석기, 운동치료기, 혈관조영장치, 혈액투석기, 레이저치료기, 약물주입기, 광선치료기, 전기자극치료기 등
PM (Patient Monitoring)	환자감시 기기 (Patient Monitoring)	Patient Monitor, Central Monitor, Fetal Monitor, Telemetry, ICP Monitor, Cardiac Output Monitor, EEG Video Monitor, Holter Monitor, Pulse Oximeter, NIBP Monitor 등
DA (Diagnosis and Analysis)	생체신호 측정, 분석 및 진단기기	CT, EKG, 초음파, 신체기능검사기기, X-ray, MRI, Gamma Camera, 소화기내시경, Auto BP 등
LA (LAboratory)	생체정보 간접 측정 및 분석 기기(혈액, 조직 등)	ABGA, Chemistry, Gamma Counter, Hematology Analyzer, Immunoassay Analyzer, 혈당측정기 등
SW (Software)	의료용 소프트웨어 (SaMD)	CAD, 3D Workstation, 초음파 분석컴퓨터 등
AS (ASsistant)	의료보조용 기기	자동약포장기, 현미경, Slide Labeller 등

현재의 의료기기는 고유한 기능에 따라 분류하고 있으므로, 보안(Security)을 위해 고려해야 할 사항은 의료기기 고유의 기능과 사용목적, 네트워크 연결 방식, 네트워크 연결 목적, 데이터 타입에 따라 보안 위험이 달라진다는 것이다. 본 논문에서는 의료기기의 고유한 기능과 더불어서 보안 위험을 평가하기 위한 분류체계를 연구한다.

3.2 의료기기 기능(Function)에 따른 분류

실제로 의료기관에서는 재료와 같은 소모성 의료기기는 자산으로 관리하지 않으며 기계나 장치들과 같은 의료기기를 자산(고정자산)으로 관리하고 있다. 고정자산으로 관리하는 의료기기도 의료기관의 규모에 따라 수천에서 수 만대에 달한다. 기구와 같은 의료기기는 소모성 자산으로 관리하는 경우도 있으며 의료기관마다 의료기기를 분류하여 기준과 체계가 모두 달라서 어느 하나로 정의하기가 어려운 것이 현실이다. 의료기기 기능에 따라 보안(Security) 위험을 분석/평가하기 위해 고려해야 할 사항은 의료기기 고유의 기능과 사용목적, 네트워크 연결 방식, 네트워크 연결 목적, 데이터 타입이다. 보안성(Security)을 고려하여 의료기기의 기능을 평가할 때 Fig 2와 같이 의료기기 연결방식(Direct Connect, Gateway, Disconnect), Data Flow(Import, Export, Mixed), Data Type(Standards, Non-Standards), 의료기기 고유기능(Therapeutic, Diagnostic, Analytical, Miscellaneous)에 따라 분류한다.



(Fig. 2) 의료기기 기능에 따른 분류

NIST는 각급 기관의 FISMA 구현을 위해 해당 표준과 지침을 전체적으로 통합하고 설명하기 위해 위험관리체계(RMF, Risk Management Framework)를 개발하고[26], 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

〈Table 3〉 의료기기 기능에 따른 평가 기준

Standard	고유기능	Potential Impact	Point	Description
Connection Type	Direct Connection	High	3	네트워크에 직접 연결된 의료기기로서 네트워크를 통한 보안위협 발생 가능성이 높음
	Connection Through Gateway	Moderate	2	게이트웨이를 통해 연결된 의료기기로서 네트워크를 통한 보안위협이 간접적으로 발생할 가능성이 있음
	Disconnection	Low	1	네트워크에 연결되지 않은 의료기기로서 네트워크를 통한 보안위협 발생 확률은 없으며, 물리적 보안위협이 발생할 가능성이 있음
Data Flow Type	Import & Export	High	3	입력과 출력 기능이 있는 의료기기로서 보안위협이 주입될 가능성이 있음.
	Import	Moderate	2	입력 기능만 있는 의료기기로서 보안위협이 주입될 가능성이 있음.
	Export	Low	1	출력 기능만 있는 의료기기로서 기기 내부에 보안위협이 주입될 가능성이 적음.
Data Type	Non-Standards	High	2	비-표준 Data Type(Raw data, Capture, log 등)의 의료기기로서 알려지지 않은 보안위협이 내재되어 있을 가능성이 높음
	Standards	Low	1	표준 Data Type(DICOM, HL7, XML 등)의 의료기기로서 표준에 따른 보안대책이 적용되어 있음.

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[27].

기능에 따른 보안위험 평가에서 기능을 분류하는 기준은 다음과 같이 보호대상인 의료기기 기능(Function) 별로 총 기능 점수를 산정하여 사용한다. FV(Function value) 는 기능(F)에 대한 평가 값의 총합(3~12)으로, 기능에 따라 영향 받는 영역(Connection Type, Data Flow Type, Data Type, Function Type)의 총합으로 산정한다. (see Equation 2)

$$V\ function value) = \sum_{=1}^{n} fi \qquad (2)$$

평가등급 구분을 위한 방안은 Table 3 와 같이 3점 분류 방식을 적용하여 각 영역별 점수를 결정한 후, 이를 합산하여 총 기능 점수를 산정하고, 산출된 총 기능 점수에 따라 평가 등급을 결정한다(see Table 3).

Function Type은 Fennigkoh와 Smith model의 Equipment function 기준을 준용한다.[28]

〈Table 4〉 Equipment function

분류	기능 정의	Point
치료	생명 유지장치	10
	수술 및 집중치료	9
	물리치료 및 치료	8
진단	수술 및 중환자실 모니터링	7
	추가적인 생리학적 모니터링 및 진단	6
분석	분석실험실	5
	실험실 부속품	4
	컴퓨터 관련	3
그외	환자 관련 및 기타	2

4. Use case

4.1 의료기기

최근 의료기기는 기술의 발전에 따라 인공지능, 빅데이터, 블록체인, 정밀의료 등 빠르게 스마트화 하고 있다. 기존의 의료기기 관리 프로그램(MEMP)으로는 스마트 의료기기를 관리하는 데 있어 한계가 존재한다. 본 논문에서 제시간 의료기기 기능에 따른 분류체계를 통해 의료기기의 보안위험 분석이 가능하며, 보

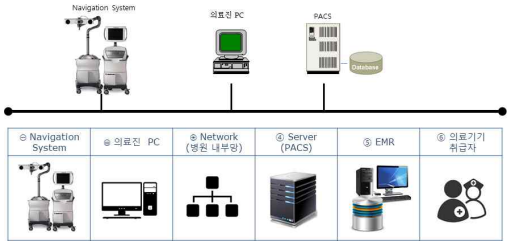
안위험 분석 결과를 포함하여 의료기기 관리 프로그램(Secure-MEMP)을 수립하고 운영함으로써 보안 위험으로부터 의료기기를 안전하게 관리할 수 있다. 주요 의료기기에 대한 위험분석 사례는 다음과 같다.

■ [Case-1] 생명유지기기 - 마취기/Patient Monitor

(Fig. 3) 생명유지기기 위험분석 Use case

① 마취기에서 생성되는 Raw Date를 “Unity ID“ 장비를 통하여 환자감시장치(Patient Monitor)로 데이터를 전송한다. ② 환자감시장치에서 생성된 데이터와 마취기에서 생성된 데이터는 중앙환자감시장치(Central Monitor)로 저장되고, ③ 병원 내부망을 통해 ④ 의료기기 인터페이스 서버로 전송된다. 의료기기 인터페이스 서버로 전송된 데이터는 ⑤ 병원정보 시스템에 연동되어 있는 전자의무기록(EMR)시스템으로 전송된다.

■ [Case-2] 수술기기 - Neuro Navigation



(Fig. 4) 수술기기 위험분석 Use case

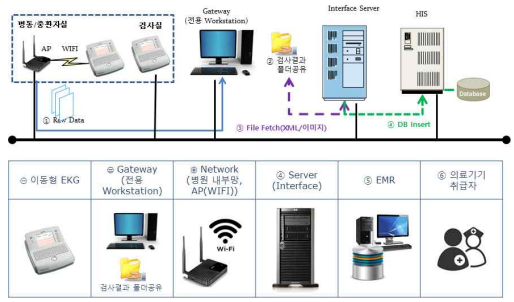
① PACS와 EMR에서 환자의 정보와 검사정보를 의료진PC로 전송한다. ② 의료진 PC에서 Neuro Navigation 전용 프로그램으로 치료정보를 생성한 후, Neuro Navigation 장비로 치료계획을 전송한다.

■ [Case-3] 치료 및 처치용 기기 - 선형가속 암치료기

(Fig. 5) 치료 및 처치용 기기 위험분석 Use case

① 환자정보와 CT 영상을 OIS(Oncology Information system) 서버로 전송한다. ② 의료진 PC에서 전용 솔루션을 통해 치료계획을 세운다. ③ 치료계획 정보를 선형가속기 암치료기로 전송하고, 선형가속기 암 치료가 이루어진다. ④ CT영상과 선형암치료기 영상은 OIS 서버로 전송하고, ⑤ OIS 서버로 전송된 PACS영상에서 환자정보와 검사정보가 Interface 서버로 전송된다. ⑥ Interface 서버 정보는 EMR로 전송 된다.

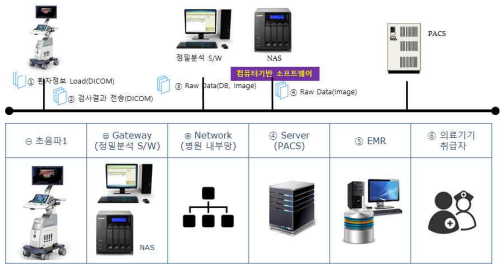
■ [Case-4] 측정, 진단 및 분석기기 - 이동식 EKG



(Fig. 6) 진단 및 분석기기 위험분석 Use case

① 검사실과 중환자실/병동에서 발생한 EKG 정보를 ② 전용 Workstation 장비로 전송하고, 검사결과 폴더에 검사정보를 저장한다. ③ 중환자실/병동에서 EKG검사정보는 무선(와이파이)를 통해서 전송된다. ④ 검사결과 폴더에 저장된 검사정보를 Interface 서버로 전송한다. ⑤ Interface 서버의 검사정보는 EMR 서버로 전송한다.

■ [Case-5] 컴퓨터기반 소프트웨어 (SaMD)



(Fig. 7) SaME 위험분석 Use case

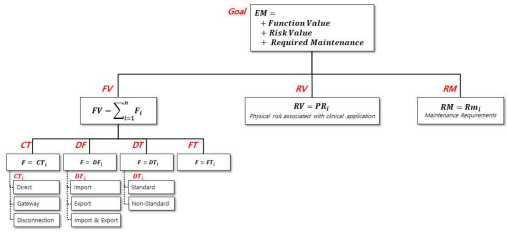
① PACS 서버에서 환자정보를 초음파장비로 전송한다. ② 초음파장비의 검사결과를 PACS 서버로 전송한다. ③ 검사정보인 Raw data(DB, Image)를 컴퓨터기반 소프트웨어인 정밀분석 게이트웨이 PC로 전송하고, 전용 저장장비에 저장한다.

의료기기 연결방식(Direct Connect, Gateway, Disconnect), Data Flow(Import, Export, Mixed), Data Type(Standards, Non-Standards), 의료기기 고유기능(Therapeutic, Diagnostic, Analytical, Miscellaneous)에 따른 분류체계를 활용하면, 본 논문에서 제시한 Use Case와 같이 의료기기의 기능에 따른 보안위협을 분석할 수 있으므로, 의료기관에서 의료기기 관리 프로그램(MEMP)을 수립할 때 의료기기에 기능에 따른 보안위험을 고려하여 보안성이 고려된 의료기기 관리 프로그램(Secure-MEMP)를 수립할 수 있을 것이다.

4.2 활용방안

본 연구결과는 우리는 연구를 위해 선택된 각 기기에 대해 위험분석을 Use case와 같이 연구하였다. 수술 및 검사 등은 임계점수가 가장 낮기 때문에 병원의 유지 관리 프로그램에서 제외할 수 있다. 본 논문에서 제안된 모델은 의료기기의 중요도를 평가하기 위해 임상 엔지니어(Fennigkoh와 Smith, 1989)가 제안한 모든 기준을 포함한다.

본 논문에서는 Fennigkoh와 Smith Model을 확장하여 기능평가 단계에 보안성을 고려할 수 있도록 의료기기 기능에 따는 분류체계를 연구하여 보안성을 평가 할 수 있는 모델을 제안하였다. 본 연구에서 제안된 모델의 한계 중 하나는 의료기기에 모델을 적용하는 과정에 보안전문가가 참여하도록 요구하고 이 과정은 전문가에게 집중적일 수 있다는 것이다. 또한 보안위협을 고려한 우선순위 결정 결과는 임상 엔지니어가 항상 수용할 수 있는 것은 아니며 기준의 가중치 및 또는 등급의 강도를 재할당해야 할 필요가 있다.



(Fig. 8) 보안성을 고려한 Fennigkoh & Smith Model

5. 결 론

스마트의료는 매우 빠른 속도로 확산되고 있다. 수많은 산업이 ICT 기술과 융합하면서 발전하고 있다. 특히, 사물인터넷(IoT) 기술의 발전으로 인하여 스마트의료는 그 확산속도가 매우 빠르다. 의료분야 특성상 사람의 생명을 다루기 때문에 정보보호는 매우 중요한 요소이다. 본 연구에서는 의료기기의 중요도에 따라 보안위험을 고려한 의료기기 관리 프로그램(Secure-MEMP) 모델을 제시한다. 이 모델은 기존 Fennigkoh와 Smith Model에서 고려되지 않았던 보안위험을 분석하고 평가하여 병원의 의료기기 관리 프로그램에 더 중요한 장치를 식별하고 포함시킨다. 본 모델은 보안위협과 물리적 위협을 평가함으로써 기기의 총 위험에 대한 보안위협을 고려한 추정치를 제공한다. 의료기기는 환자에 대한 생명과 밀접하게 연결될 수 있기 때문에 보안관리의 중요성이 지속적으로 증가하고 있다. 최근 발전하고 있는 다양한 의료기기들은 기능적으로 많은 발전이 이루어졌으나 이로 인하여 의료기기에서 발생할 수 있는 잠재적인 보안위협도 함께 증가하고 있다. 의료기기 또는 의료장비는 의료분야에서 중요한 역할을 하지만, 적절하게 사용되거나 유지 및 관리되지 않을 경우 해를 끼칠 수도 있다. 본 논문에서 제시한 모델을 활용하여 병원의 임

상 엔지니어링 부서는 보안위협을 고려하여 안전하고 신뢰할 수 있는 의료 장비 관리 프로그램 수립 및 규제할 것으로 기대한다.

참고문헌

[1] T. Y. Kim, S. K. Y. J. J. Jung and E. J. Kim, “Multi-Hop WBAN Construction for Healthcare IoT Systems”, 2015 International Platform Technology and Service(PlatCon), pp. 27-28, Jan. 2015.

[2] Y. S. Jeong, “An Efficient IoT Healthcare Service Management Model of Location Tracking Sensor”, Journal of Digital Convergence, Vol. 14, No. 3, pp. 261-267, Mar. 2016.

[3] B. Zhang, X. W. Wang, M. Huang, “A data replica placement scheme for cloud storage under healthcare IoT environment”, 2014 11th International Conferenceon Fuzzy Systems and Knowledge Discovery (FSKD), pp. 542-547, Aug. 2014.

[4] Y. S. Jeong, “Design of Prevention Model according to a Dysfunctional of Corporate Information,”Journal of Convergence Soceity for SMB, Vol. 6, No. 2, pp. 11-17, Jun. 2016.

[5] Y. S. Jeong, “Tracking Analysis of User Privacy Damage using Smartphone”, Journal of Convergence Society for SMB, Vol. 4, No. 4, Dec. 2014.

[6] Y. S. Jeong, “Design of Security Model for Service of Company Information,” Journal of Convergence Soceity for SMB, Vol. 2, No. 2, pp. 43-49, Nov. 2012.

[7] J.A. Hansen, N.M. Hansen A taxonomy of vulnerabilities in implantable medical devices Proc. of the Second Annual Workshop on Security and Privacy in Medical and Home-care Systems, SPIMACS ’10, ACM, New York, USA , pp. 13-20, 2010.

[8] Carmen Camara, Pedro Peris-Lopez, Juan E.Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey", Journal of Biomedical Informatics, Volume 55, June 2015, Pages 272-289.

[9] U.S. Food and Drug Administration (FDA), Medical Device Safety. <http://wireless.fcc.gov/services/index.htm?job=service_bandplan&id=medical_implant> (consulted on November of 2013).

[10] HIPPA, Security standards: technical safeguards 2(4) (2007) 1?17. Google Scholar

[11] S. Shivshankar, K. Summerhayes Challenges of conducting medical device studies Inst. Clin. Res, 2007.

[12] K. Fu Inside risks: reducing risks of implantable medical devices ACM Commun., 52 (6) (2009), pp. 25-27.

[13] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W.H. Maisel, Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses, in: Proc. of the 29th Annual IEEE Symposium on Security and Privacy, 2008, pp. 129?142.

[14] C. Li, A. Raghunathan, N.K. Jha, Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system, in: 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom), June 2011, pp. 150?156.

[15] Medtronic, Implantable pacemaker and defibrillator information. consulted on April 2015.

[16] TheVerge, Dick Cheney had the Wireless Disabled on his Pacemaker to Avoid Risk of Terrorist Tampering, 2013.

[17] FDA, “Postmarket Management of Cybersecurity in Medical Devices”, 2016.12.28.

[18] N. Paul et al., “A Review of the Security of

Insulin Pump Infusion Systems," Journal of Diabetes Science and Technology, 5(6):1557-62, November 2011.

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

[20] S Taghipour, D Banjevic and AKS Jardine, "Prioritization of medical equipment for maintenance decisions,", Journal of the Operational Research Society, Volume 62, Issue 9, pp. 1666 - 1687, September 2011.

[21] Fennigkoh L and Smith B. Clinical equipment management.JCAHO PTSM Series 2:5 - 14. Cited on pages(24), January 1989.

[22] D. Kim, J. Choi and K. Han, "Medical Device Safety Management Using Cybersecurity Risk Analysis," in IEEE Access, vol. 8, pp. 115370-115382, 2020, doi: 10.1109/ACCESS.2020.3003032.

[23] Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem.

[24] US Food and Drug Administration [homepage on the Internet] Is The Product A Medical Device? FDA; 2014.

[25] International Medical Device Regulators Forum . "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations. IMDRF Software as a Medical Device (SaMD) Working Group; 2014, Accessed June 9, 2015.

[26] Ross RS, Johnson LA. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; 2010.

[27] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J, Gulick J. Guide for Mapping Types of Information and Information Systems to Security Categories. NIST. 2008.

[28] World Health Organizaiton, "Introduction to medical equipment inventory management," WHO Medical device technical series, June 2011

[29] Kim, Dw., Choi, Jy. & Han, Kh. Risk management-based security evaluation model for telemedicine systems. BMC Med Inform Decis Mak 20, 106 (2020). https://doi.org/10.1186/s12911-020-01145-7.

[30] IHE PCD Technical Committee, "Medical Equipment Management (MEM): Medical Device Cyber Security ?Best Practice Guide," IHE International, July1, 2015.

〔저자소개〕

김 동 원 (Dong-Won Kim)
2009년 2월 서울과학기술대학교 학사
2012년 2월 건국대학교 석사
2021년 2월 고려대학교 박사
2017년~현재 건양대학교 사이버보안공학과 조교수
email : blast@konyang.ac.kr