연세대학교 YONSEI UNIVERSITY

CIA Triad 확장모델 및 Threat 모델링에 기반한 소프트웨어 의료기기 사이버보안 프레임워크

한혜리[1*], 구성욱[2], 장원석[3]
연세대학교 대학원 의료기기산업학과

A Cybersecurity Framework for Software as a Medical Device: Integrating Alternative CIA Triad Models and Threat Modeling Methodologies

Hyeri Han[1*], Sung Uk Kuh[2], Won Seok Jang[3]
Department of Medical Device Engineering and Management, Yonsei University College of Medicine, Korea
*rihan@yonsei.ac.kr

Abstract

As cybersecurity threats continue to rise, highlighted by an average financial loss of $10.93 million per data breach in the healthcare sector, marking the highest figure for 13 consecutive years, the importance and urgency of cybersecurity in the SaMD domain have become more prominent. This research introduces a hybrid Cybersecurity Framework (hCSF) that can be applied throughout the entire lifecycle of SaMD, based on the alternative CIA Triad model and threat modeling methodologies. The proposed framework integrates CIA Triad models expanded such as the Parkerian Hexad and McCumber Cube, along with various threat modeling approaches including STRIDE, LINDDUN, and OCTAVE. This integration enables comprehensive management of cybersecurity requirements from technical, administrative, and operational perspectives. By implementing the principle of Security by Design, the framework would facilitate the inclusion of security considerations from the early stages of software design and development, offering a more cost-effective and efficient security approach compared to reactive methods. The study confirms that the proposed framework can be flexibly configured into various combinations tailored to the intended use, principle of operation, and cybersecurity regulatory policies of the target market for SaMD. Moving beyond the traditional checklist approach to technical cybersecurity requirements, this study presents a new framework that identifies cybersecurity threats and implements response strategies throughout the SaMD lifecycle. It provides a new theoretical perspective and direction in the field of SaMD cybersecurity. Ultimately, the research aims to contribute to the improvement of global competitiveness in the SaMD sector, serve as a foundational reference for cybersecurity policy development, and support the establishment of safer and more reliable digital healthcare and SaMD cybersecurity management strategies.

1. 연구 배경

고령화 및 만성질환의 유병률 증가, 환자맞춤형 의료서비스에 대한 수요 증가 및 클라우드 기반의 서비스형 소프트웨어(Software as a Service, SaaS) 플랫폼의 도입 증가 등과 같은 주요한 동인에 힘입어 디지털 헬스분야 기술의 급속한 발전과 함께 소프트웨어 의료기기(Software as a Medical Device, SaMD)의 활용이 크게 증가하고 있다[1]. 소프트웨어 의료기기(SaMD)는 의료 목적으로 범용 장비에서 사용되는 독립형 소프트웨어를 뜻하며, 일반적으로 진단, 치료 및 모니터링 등 다양한 의료 서비스를 제공한다. 해당 글로벌 시장 규모는 2025년 18억 달러에서 2033년 약 50억 달러의 가치가 있을 것으로 예상되며, 2033년까지의 예측 기간 동안 13.6%의 연평균성장률(Compound Annual Growth Rate, CAGR)로 성장할 것으로 예상된다[2].

한편 소프트웨어 의료기기(SaMD)의 확산은 의료데이터 보안 및 개인정보 보호에 대한 우려와 사이버보안 위협에 대한 취약점 증가로 이어지고 있으며, 미국 식품의약국(Food and Drug Administration, FDA)은 2023년 의료기기 사이버보안은 곧 환자 안전이며, 사이버보안 사고는 의료기기의 가용성과 성능에 심각한 위협이 될 수 있음을 시사한 바 있다[3]. 특히 환자 데이터 유출, 무단 접근, 의료기기 기능 변조 등의 사이버 위협이 증가하고 있으며, 이는 환자 안전(Patient Safety)과 직결되는 심각한 문제이다. 또한 국제 의료기기 규제당국자 포럼(International Medical Device Regulators Forum, IMDRF)은 소프트웨어 의료기기(SaMD)의 사이버보안이 제품 수명주기 전반에 걸쳐 고려되어야 할 핵심 요소임을 강조하고 있으나[4], 현재 지속적으로 발전하고 있는 소프트웨어 의료기기 (SaMD)와 사이버 위협을 고려하여 대응할 수 있는 사이버보안 프레임워크는 부족한 실정이다. 기존의 의료기기 사이버보안 가이드라인은 주로 하드웨어를 동반한 종속형 소프트웨어(Software in Medical Device, SiMD)와 혼용되어 개발되거나 기술적 보안 요구사항 체크리스트 방식에 국한되었다는 한계를 가지고 있다.

아울러, 최근 발표된 학술지에 따르면 2023년 의료 분야에서 발생한 대규모 보안침해 사례는 725건으로 보고되었으며, 의료 데이터 침해에 따른 사이버 보안사고가 매년 증가하는 추세이며, 2023년에는 매일 평균 2건의 대규모 의료 데이터 침해가 발생하였다[5]. 시간이 지남에 따라 더욱 정교해지는 사이버 공격에 대처하기 위한 효과적인 방법론의 일환으로 위협 모델링 기반의 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크를 통한 접근방식은 디지털 헬스분야의 기술 발전에 발맞춘 환자 안전의 확보 및 의료 시스템의 신뢰도 유지를 나아가 산업 및 국가의 경쟁력을 위해 중요한 과제로 대두되고 있다.

2.연구 방법

본 연구에서는 확장된 CIA Triad 모델 및 위협 모델링 기반의 소프트웨어 의료기기(SaMD)에 관한 사이버보안

프레임워크를 제안하기 위해 다음과 같은 연구 방법을 활용한다. 우선 국내·외 문헌조사를 통해 정보보안 및 사이버보안에 대한 내용을 전반적으로 파악하고, 관련된 국내외 사이버보안 정책자료 및 규제동향을 검토하여 사이버보안 관련 요구사항과 위협 모델링 적용사례 등을 면밀하게 분석한다. 또한, 적용 가능한 대표적인 보안 목표 모델 및 위협 모델링 방법론 등을 수집하고, 수명주기 전반에 걸쳐 사용할 수 있는 프레임워크를 분석 및 제시한다. 현재까지 소프트웨어 의료기기(SaMD) 분야에서 CIA Triad 이외의 보안 모델과 위협 모델링의 적용 사례가 다소 제한적이므로 다양한 분야의 적용 사례를 함께 조사하여 적절하게 조정하는 방안을 모색하도록 한다. 더불어, 의료기기 사이버보안 국제표준 등과의 조화를 위해 국제 의료기기 규제 당국자 포럼(IMDRF)과 국제 표준화 기구(ISO), 국제 전기기술 위원회(IEC) 등과 같은 기관의 관련된 발행자료를 심층적으로 이해하고 적용하여 새로운 프레임워크를 제안하고, 사례 연구를 수행하도록 한다.

3. 연구 결과

본 연구에서는 확장된 CIA Triad 모델과 위협 모델링 방법론을 기반으로 소프트웨어 의료기기(SaMD)의 수명주기 전반에 걸쳐 활용할 수 있는 하이브리드 사이버보안 프레임워크(hybrid Cybersecurity Framework, hCSF)를 개발하였다. 개발된 프레임워크는 기존의 전통적이고 획일화된 의료기기 위험관리 접근방식에서 벗어나 Parkerian Hexad 모델 및 McCumber Cube 모델 등의 CIA Triad 확장모델과 STRIDE, LINDDUN, OCTAVE, PASTA 및 VAST Threat Modeling 등과 같은 다양한 위협 모델링 방법론을 통합하여 설계되었으며, 소프트웨어 의료기기(SaMD)의 의도된 사용목적, 작용원리 및 진출하고자 하는 국가의 사이버보안 규제정책 또는 조직의 보안정책 등에 따라 다양한 결합으로 구성될 수 있는 유연성을 제공한다.

그림1. 하이브리드 사이버보안 프레임워크(hCSF)

특히 진료기록, 의료영상, 생체신호, 병리검사, 유전정보 등과 같은 민감한 개인 의료데이터를 수집, 전송, 저장 및 분석 처리하는 소프트웨어 의료기기(SaMD)의 특성을 고려하여 환자의 개인정보보호와 환자안전이라는 핵심 보안 요구사항을 동시에 실현할 수 있도록 설계되었으며, 설계 및 개발 초기 단계부터 보안 요소를 고려하는 Security by Design 원칙을 구현할 수 있어 품질비용 측면에서 효율적이고 효과적인 보안체계 구축을 가능하게 한다.

본 연구에서 제안한 하이브리드 사이버보안 프레임워크(hCSF)를 활용하여 설계한 예시로써 여러 확장된 CIA Triad 모델과 위협 모델링 방법론 중에서 McCumber Cube와 LINDDUN Threat Modeling을 선택적으로 결합하였다. 기본적으로 McCumber Cube 모델은 기밀성, 무결성 및 가용성과 같은 보안 목표(Security Goals)와 전송, 저장 및 처리와 같은 정보 상태(Information State) 그리고 기술, 정책과 관행, 교육훈련과 같은 보안 조치(Security Measures)라는 3가지 축으로 구성된 3차원 큐브 형태의 모델이다. 보안 위협 또는 취약점, 대응방안 등을 다각도로 분석하기에 적합하다. 한편, LINDDUN위협 모델링은 개인정보 보호분야에 중점을 두고 있기 때문에 개인 의료데이터와 관련된 보안을 위해 활용하기 적합하다.

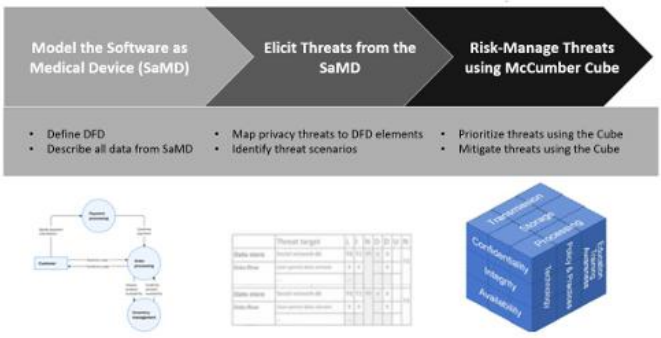

그림2. McCumber Cube + LINDDUN 프레임워크 프로세스

연결성(Linkability), 식별성(Identifiability), 부인 방지(Non-repudiation), 탐지성 (Detectability), 정보 공개(Disclosure of information), 인식 부족(Unawareness), 규정 미준수(Non-Compliance)와 같은 7가지 위협 유형에 대해 6단계의 프로세스를 따르는 방식이며, 개인정보 보호통제를 위한 체계적인 접근방식을 제공한다. 따라서 McCumber Cube + LINDDUN 프레임워크는 사이버보안 및 개인정보 보호를 동시에 만족할 수 있으며, 상기 그림 2와 같이 크게 3가지 단계의 프로세스로 이루어진다.

4. Acknowledgements

이 연구는 연세대학교 대학원 의료기기산업학과의 지원을 받아 수행하였음. (I804:11046-000000560742, 2025)

5.참고 문헌

[1] IQVIA, Digital Health Trends 2024, 2024
[2] Market.US, Software as a Medical Device (SaMD) Market Research Report, 2024
[3] Food and Drug Administration (FDA), Medical Device Cybersecurity Helping to Keep Patients and Medical Devices Safe, 2023
[4] International Medical Device Regulators Forum (IMDRF), IMDRF/CYBER WG/N60: Principles and practices for medical device cybersecurity, 2020
[5] The Health Insurance Portability and Accountability Act Journal, 2024 Healthcare Data Breach Report, 2025