코드 생성에 대한 부적절한 제어 탐지 기술에 관한 연구

김남현[1], 구지현[2], 손민지[3], 김하원[4], 고광만[5]
[1,5]상지대학교 컴퓨터공학과, [2]상지대학교 소프트웨어학과, [3,4]한국폴리텍대학교
202048004@sj.sangji.ac.kr, akswk17@gmail.com, yeondugolae@gmail.com ,kkman@sangji.ac.kr

A Study on Detection Technique of Improper Control of Code Generation

Nam-Hyun Kim[1], Jee-Hyun Koo[2], Minji Son[3], Ha-won Kim[4], Kwang-Man Ko[5]
[1,5]Dept. of Computer Engineering, [3,4]Korea Polytechnics [2]Dept. of Software, Sang-Ji University

요 약

디지털 헬스케어에서 의료기기 소프트웨어의 보안은 환자 데이터 보호와 기기 기능 유지에 있어 매우 중요하다. 현재 많은 의료기기 소프트웨어는 보안 취약점에 노출되어 있으며, 특히 CWE-94(코드 삽입)와 Hollowing Process 같은 공격 기법이 문제로 대두되고 있다. 이러한 취약점은 보안 솔루션의 우회를 가능하게 하며, 의료 기기의 무결성과 환자 안전을 위협할 수 있다. 본 논문에서는 동적/정적 리버싱 도구를 활용하여 이러한 취약점을 탐지하고 분석하는 방법을 제시 및 진행중이며 이를 통해 의료 기기 소프트웨어의 보안을 강화하는 데 기여할 수 있다.

1. 서론

디지털 헬스케어 분야에서 의료 기기의 소프트웨어 의존도가 증가함에 따라 소프트웨어 보안이 중요한 이슈로 떠오르고 있다. 그 중 2023년도 CWE(Common Weakness Enumeration)에서 발표한 소프트웨어 취약점 Top 25중 CWE-94(코드 삽입)와 그에 포함되는 Hollowing Process가 주는 취약점은 의료 기기 소프트웨어의 무결성을 위협하여 환자 데이터와 기기 기능을 크게 손상시킬 수 있. 본 논문에서는 CWE-94와 Hollowing Process을 중심으로 이러한 위협을 이해하고, 동적/정적 리버싱 도구를 통해 이를 탐지하고 방지하는 능력을 향상시키는 데 초점을 두었고 이를 통해 의료 기기 소프트웨어의 보안을 강화하고 환자 데이터 및 의료 기기의 소프트웨어 안전성을 향상시키는 것을 목표로 하고 있다..

2. 관련 연구

2-1. 디지털 헬스케어 보안 위협

디지털 헬스케어라는 의료영역에 정보통신기술(ICT)을 융합해 개인 건강과 질병에 맞춰 필요한 의료서비스나 건강관리 서비스를 제공하는 산업 또는 기술을 말한다. 이에 따른 2021년 한국 인터넷 진흥원에서 발표한 소프트웨어 보안 약점 진단 가이드에 따르면 디지털 헬스케어에 관련된 보안 위협에 유형은 인증 및 허가, 암호, 데이터 보안 및 안전한 통신, 안전한 기기 관리 및 물리적 보호 등 4개의 보안위협 유형으로 정의한다.

<표 1> 디지털 헬스케어 보안 위협 유형

유형	정의
인증 및 허가 (Authentication & Authorization)	사용자나 기기의 신원을 확인하고, 역할에 따라 적절한 접근 권한을 부여하는 과정
암호 (Password)	환자 정보 등의 민감한 데이터를 무단 접근, 유출, 변조로부터 보호하는 조치
데이터 보안 및 안전한 통신 (Data Security & Secure Communication)	네트워크 상의 데이터를 암호화하여 전송 중 도청이나 변조를 방지하는 통신 방식입니다.
안전한 기기 관리 및 물리적 보호 (Secure Device Management & Physical Protection)	의료 기기를 디지털 및 물리적으로 안전하게 유지하고 보호하는 관리 및 보안 조치입니다.

2-2. CWE-94와 Hollowing Process

CWE-94(코드 삽입)는 소프트웨어의 코드 생성 과정에서 적절한 제어가 이루어지지 않아, 악의적인 코드가 삽입될 수 있는 취약점을 의미하며 의료 기

기 소프트웨어에서 CWE-94가 악용될 경우, 공격자는 시스템의 권한을 탈취하거나 환자 데이터를 조작할 수 있습니다. 2020년 SolarWinds의 Orion 소프트웨어 업데이트 과정에 악성 코드를 삽입하여 수많은 기업과 정부 기관의 시스템에 침투한 사례가 보고되었다. 만약 이러한 공격이 의료기기 소프트웨어에 발생한다면, 의료 데이터 유출뿐만 아니라 기기의 오작동을 초래할 수 있다. 또한, 코드 삽입의 기법의 일종인 Hollowing Process는 악성 코드가 정상적인 프로세스를 가로채어 실행되는 기법으로, 이는 탐지가 어렵고 보안 솔루션을 우회할 수 있다. Hollowing Process는 의료기기에서 중요한 기능을 하는 소프트웨어에 적용될 경우, 시스템 운영에 심각한 문제를 일으킬 수 있다.

2023 CWE Top 25

Rank	ID	Name	Score	CVEs in KEV
1	CWE-787	Out-of-bounds Write	63.72	70
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.54	4
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	34.27	6
4	CWE-416	Use After Free	16.71	44
23	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.30	6
24	CWE-863	Incorrect Authorization	3.16	0
25	CWE-276	Incorrect Default Permissions	3.16	0

(그림 1) 2023 CWE TOP 25

이를 해결하기 위해 동적/정적 각각의 역공학 도구를 활용한 분석과 취약점 탐지가 중요하며, 입력 값 검증 및 메모리 모니터링과 같은 기법을 통해 소프트웨어의 보안 취약점 보안에 대해 연구한다.

3. 코드 삽입 탐지 방안

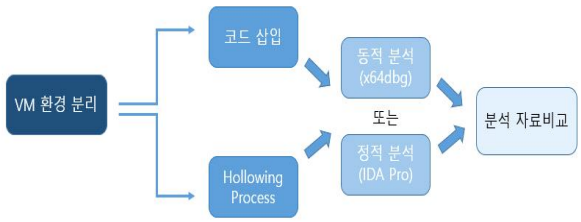
3-1. 코드 삽입과 Hollwoing Process 대상 및 구성

코드 삽입(CWE-94)과 할로잉 프로세스를 분석하기 위해 윈도우 환경에서 실험을 진행하였으며, 안전한 실험을 위해 가상 머신을 활용하여 환경을 분리했다. 이를 통해 윈도우와 리눅스 환경을 각각 격리하여 다양한 운영체제에서 보안 취약점을 분석할 수 있도록 설정하였다. 현재, 윈도우 환경에서 실험이 이루어지고 있으며, x64dbg와 IDA Pro를 사용하여 코드 삽입 기법의 일종인 할로잉 프로세스를 탐지하고 분석하는 것을 목표로 연구를 진행하고 있다. 가상머신을 활용한 환경 분리를 통해 실제 시스템에 미치는 영향을 최소화하면서도 공격 기법과 보안 취약점을 효율적으로 연구할 수 있. 이 실험 환경은 코드 삽입 및 프로세스 할로잉 기법이 의료 기기 소프트웨어에 미치는 영향을 분석하고, 이를 방지하기 위한 보안 도구의 사용에 중점을 두고 있다.

<표 2> 연구 대상 및 환경

항목	세부 내용
실험 환경	Windows, Linux (VM을 통한 환경 분리)
사용 도구	x64dbg, IDA Pro
분석기법	코드 삽입(CWE-94), 프로세스 할로잉

3-2. 실험 절차 및 학습 방법



(그림 2) 코드삽입과 할로잉 프로세스 감지 실험 절차

가상머신을 이용한 환경 분리 후, 악성 코드 예제를 IDA Pro 또는 x64dbg로 분석하였다. 이 분석은 윈도우와 리눅스 환경에서 각각 진행되었으며, 운영체제에 따라 역공학(리버싱) 도구의 결과 값에 차이가 나타났다. 정상 프로세스와 악성 프로세스의 결과 값을 비교하여, 동적 및 정적 분석 도구의 사용법을 익히고 취약점 탐지 능력을 향상시키는 것을 중점적으로 진행하고 있다..

4. 결론

본 논문에서는 윈도우즈와 리눅스 환경에서 코드 삽입(CWE-94)과 할로잉 프로세스를 분석하였으며, IDA Pro와 x64dbg 같은 분석 도구를 활용하였다. 본 논문을 통해 보안 분석 도구의 활용 능력과 취약점 탐지 기술을 연구하고 있으며, 앞으로 더 다양한 보안 기법과 공격 시나리오를 연구할 예정이다.

참고문헌

[1] 한국인터넷진흥원 “디지털 헬스케어 보안모델”, 2021.12

[2] MITER Corporation “2023 CWE TOP 25 List”.2023.11