소프트웨어 취약점 분석 장치 및 방법

대표발명자 : 윤주범 교수

소프트웨어 취약점 분석 장치 및 방법

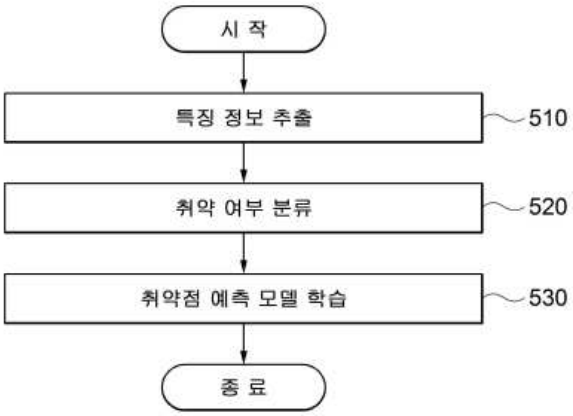
□ 기술개요

○ 본 발명은 소프트웨어에 포함된 취약점(vulnerability)을 분석하기 위한 기술임

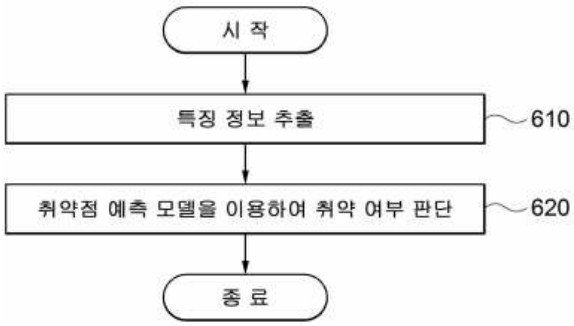
○ 소프트웨어 취약점 분석 장치는 소프트웨어 바이너리 파일에 대한 특징 정보를 추출하고, 인공 신경망 기반의 취약점 예측 모델을 이용하여 특징 정보로부터 소프트웨어 바이너리 파일의 취약 여부를 판단함

○ 취약점 예측 모델은 사전 수집된 복수의 바이너리 파일 각각에 대한 특징 정보 및 취약 여부 분류 결과를 이용하여 사전 학습되며, 소프트웨어 바이너리 파일에 대한 특징 정보는 소프트웨어 바이너리 파일이 실행될 때 호출되는 함수들에 대한 정보를 포함함

□ 대표도면



<취약점 예측 모델 학습 방법의 순서도>



<소프트웨어 취약점 분석 방법의 순서도>

□ 기술의 특징 및 우수성

○ 본 기술은 사전 수집된 소프트웨어 바이너리 파일에서 추출된 특징을 이용하여 사전 학습되는 인공 신경망 기반의 예측 모델을 이용하여 소프트웨어 바이너리 파일에 포함된 취약점 분석을 수행함으로써, 소프트웨어에 대한 소스 코드 없이도 바이너리 파일만을 이용하여 정확하고 신속한 취약점 분석이 가능함

[표] 기술의 특징 및 우수성

종래기술 문제점	• 종래 소프트웨어 취약점 분석 기술은 분석 시간이 많이 소요되며 소프트웨어에 대한 소스 코드가 제공되지 않을 경우 분석 정확도가 높지 않거나 분석이 불가능함
해결방안	• 사전 수집된 소프트웨어 바이너리 파일에서 추출된 특징을 이용하여 인공 신경망 기반의 예측 모델을 학습시킨 후, 학습된 예측 모델을 이용하여 분석 대상 소프트웨어 바이너리 파일에 대한 취약점 분석을 수행함
기술의 특징 및 우수성	• 취약점 분석을 위해 **소프트웨어에 대한 소스 코드가 요구되지 않으며, 역어셈블(disassemble)과 같이 바이너리 파일에 대한 별도의 변환 과정 없이 바이너리 파일 자체를 이용한 분석이 가능**함

□ 기술의 효과

○ 소프트웨어 바이너리 파일에서 추출한 특징을 이용하여 학습된 인공 신경망 기반의 예측 모델을 이용하여 취약점 분석을 수행함으로써 소스 코드 없이 바이너리 파일만으로도 정확하고 신속한 취약점 분석이 가능함

□ 기술의 완성도(TRL)

기초 연구 단계		실험 단계		시작품 단계		제품화 단계		사업화
기본원리 파악	기본개념 정립	기능 및 개념 검증	연구실환경 테스트	유사환경 테스트	파일럿현장 테스트	상용모델 개발	실제 환경 최종테스트	상용운영
			●					

□ 기술 키워드

한글키워드	소프트웨어, 취약점, 바이너리, 특징, 신경망
영문키워드	software, vulnerability, binary, feature, neural network

□ 기술의 적용분야

○ 본 기술은 안전한 소프트웨어 개발을 위해 소프트웨어에 존재할 수 있는 잠재적인 취약점을 탐지하는 소프트웨어 취약점 분석 서비스에 적용 가능함

[표] 적용분야

소프트웨어 개발 보안
소프트웨어 취약점 분석

□ 기술경쟁력

○ 취약점 분석을 위해 소프트웨어의 소스 코드가 요구되지 않으며, 종래 취약점 분석 기술과 같이 소프트웨어의 바이너리 파일을 CPU 구조에 따라 달라지는 어셈블리 코드로 변환할 필요가 없으므로, 상이한 CPU 환경에서도 정확한 취약점 분석이 가능함

□ 기술실시에 따른 기업에서의 이점

○ 종래 취약점 분석 기술에 비해 소스 코드를 요구하지 않으며, 정확성을 보장하면서도 신속하고 효율적인 취약점 분석 서비스 제공이 가능하게 되므로 시장 경쟁력 확보 가능

[표] 소프트웨어 취약점 분석 분야의 SWOT 분석

강점(Strength)	약점(Weakness)
• 알려진 소프트웨어 취약점에 대한 데이터베이스 구축이 활성화 되어 있음 • 국가 정보화사업으로 개발되는 소프트웨어에 대한 시큐어 코딩 의무화	• 핵심 원천기술 부족 • 전문 인력 부족
기회요인(Opportunity)	**위협요인(Threat)**
• DDoS 공격, 해킹 등과 같이 소프트웨어 취약점에 대한 공격 사례 증가 • ICT 및 IoT 기술 발달로 인한 오픈 소스 소프트웨어 활용이 증가함에 따라 시큐어 코딩(secure coding)의 중요성 증가	• 국내 취약점 분석 업체들 사이의 가격 경쟁 심화 • 국내 취약점 분석 시장 협소

□ 특허현황

구분	발명의 명칭	출원번호 (출원일)	등록번호 (등록일)	출원국가
1	소프트웨어 취약점 예측 모델 학습 장치 및 방법, 소프트웨어 취약점 분석 장치 및 방법	10-2018-0142533 (2018.11.19.)	10-1963756 (2019.03.25.)	한국