소프트웨어 취약점 분석 장치 및 방법

대표발명자 : 윤주범 교수

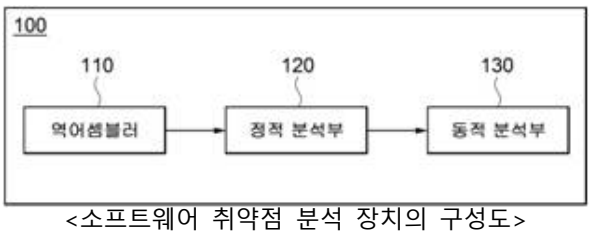
소프트웨어 취약점 분석 장치 및 방법

□ 기술개요

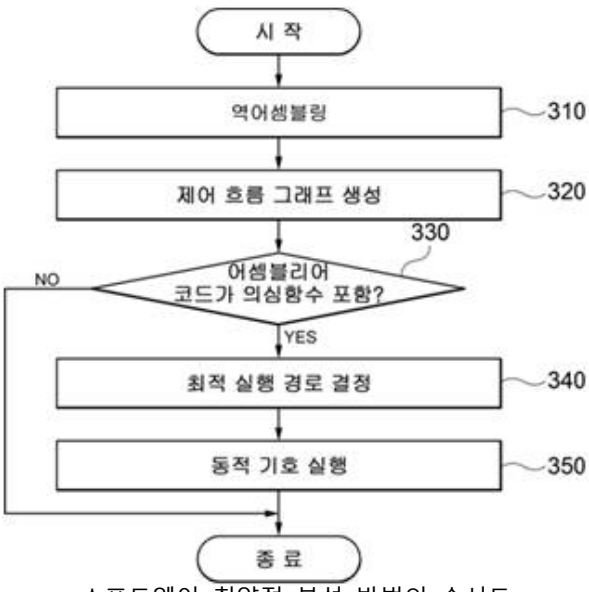
○ 본 발명은 소프트웨어에 포함된 취약점(vulnerability)을 분석하기 위한 기술임

○ 소프트웨어 취약점 분석 장치는 소프트웨어 바이너리 파일에 대한 어셈블리어 코드를 생성하는 역어셈블러(110), 어셈블리어 코드에 대한 제어 흐름 그래프(control flow graph)를 생성하여 문자 검색을 통해 어셈블리어 코드가 사전 정의된 의심 함수를 포함하고 있는지 여부를 판단하는 정적 분석부(120) 및 의심 함수가 포함되어 있는 경우, 제어 흐름 그래프에 기초하여 의심 함수를 실행하기 위한 최적 실행 경로를 결정하고, 소프트웨어 바이너리 파일을 이용하여 최적 실행 경로에 대한 동적 기호 실행(concolic execution)을 수행하는 동적 분석부(130)를 포함함

□ 대표도면



<소프트웨어 취약점 분석 장치의 구성도>



<소프트웨어 취약점 분석 방법의 순서도>

□ 기술의 특징 및 우수성

○ 본 기술은 소프트웨어의 바이너리 파일을 역어셈블하여 생성된 어셈블리어 코드를 바탕으로 작성된 제어 흐름 그래프를 이용하여 취약점 의심 함수를 실행하기 위한 최적 실행 경로를 결정하고, 결정된 최적 실행 경로에 대한 동적 기호 실행(concolic execution)을 수행함으로써 소스 코드 없이 유포되는 소프트웨어에 대한 취약점 분석이 가능함

[표] 기술의 특징 및 우수성

종래기술 문제점	• 종래 소프트웨어 취약점 분석 기술은 소프트웨어에 포함된 분기문과 반복문에 의해 발생하는 경로 폭발(path explosion) 문제로 인하여 소프트웨어에 포함된 모든 명령어를 점검하지 못하거나 분석에 지나치게 오랜 시간이 요구되므로, 분석 정확성과 효율성이 저하되는 문제점이 있음
해결방안	• 소프트웨어 바이너리 파일을 역어셈블하여 어셈블리어 코드를 생성하고, 생성된 어셈블리어 코드에 대한 제어 흐름 그래프(control flow graph)를 생성한 후, 문자 검색을 통해 어셈블리어 코드에 사전 정의된 의심 함수가 포함되어 있는지 여부를 판단하여, 의심 함수가 포함되어 있는 경우, 제어 흐름 그래프를 이용하여 의심 함수에 대한 최적 실행 경로를 결정하여 최적 실행 경로에 대한 동적 기호 실행을 수행함
기술의 특징 및 우수성	• 소프트웨어 바이너리 파일에 포함된 의심 함수로의 최적 실행 경로를 결정하여 결정된 최적 실행 경로에 대해서만 취약점 분석을 수행하므로 **경로 폭발 문제를 해결**할 수 있으며, 이에 따라 **취약점 분석을 위해 요구되는 시간을 줄일 수 있음**

□ 기술의 효과

○ 취약점 의심 함수를 실행하기 위한 최적 실행 경로에 대해서만 동적 분석을 수행하고, 최적 실행 경로를 제외한 나머지 실행 경로에 대한 동적 분석을 생략함으로써 분기문과 반복문에 의해 발생하는 경로 폭발 문제를 해결함과 동시에 효율적인 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, 제어 흐름 그래프
영문키워드	software, vulnerability, binary, control flow graph, CFG

□ 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

○ 알려진 취약점 의심 함수에 대한 최적 실행 경로에 대해서만 동적 기호 실행을 통한 동적 분석을 수행함으로써 불필요한 동적 기호 실행 횟수를 줄일 수 있으며, 이를 통해 분석의 신속성과 효율성을 향상시키면서 분석 정확성을 확보할 수 있음

□ 기술실시에 따른 기업에서의 이점

○ 종래 취약점 분석 기술에 존재하는 경로 폭발 문제를 해결함에 따라 분석 정확성을 확보하면서 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)	출원 국가
1	소프트웨어 취약점 분석 장치 및 방법	10-2018-0133775 (2018.11.02.)	10-1963752 (2019.03.25.)	한국