프로세스 중단 없는 메모리 랜덤화

대표발명자 : 윤주범 교수

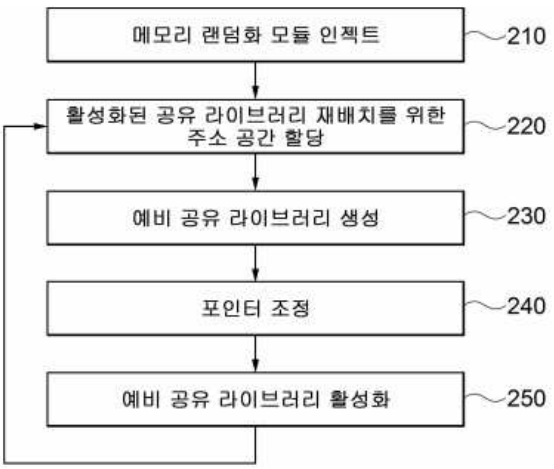
프로세스 중단 없는 메모리 랜덤화

□ 기술개요

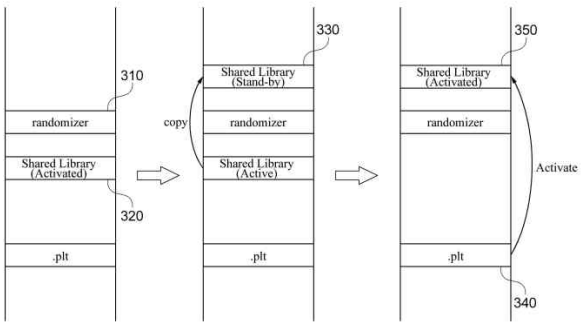
○ 본 발명은 메모리 랜덤화를 통해 코드 재사용(code reuse) 공격, ROP(Return-Oriented Programming) 공격 등과 같은 메모리 공격을 방어하기 위한 기술임

○ 실행 중인 대상 프로그램에 메모리 랜덤화 모듈을 인젝트(inject)하여 메모리 랜덤화 모듈이 대상 프로그램에 의해 이용되는 공유 라이브러리를 임의의 메모리 주소 공간으로 복사하여 예비(stand-by) 공유 라이브러리를 생성하고, 공유 라이브러리에 대한 포인터를 수정한 후 예비 공유 라이브러리를 활성화하는 과정을 대상 프로그램 실행 중에 반복 수행하도록 함

□ 대표도면



<메모리 랜덤화 방법의 순서도>



<메모리 랜덤화의 예시도>

□ 기술의 특징 및 우수성

○ 본 기술은 대상 프로그램의 실행 중 인젝트되는 메모리 랜덤화 모듈을 이용하여 재컴파일이나 프로세스 중단 없이 메모리 랜덤화가 가능하도록 함으로써, 미션 크리티컬 애플리케이션(mission critical application)과 같이 프로세스

중단 없이 수행되어야 하는 응용 프로그램에 대한 메모리 공격을 방어할 수 있음

[표] 기술의 특징 및 우수성

종래기술 문제점	• 메모리 공격 방어를 위한 종래 메모리 랜덤화 기술은 메모리 랜덤화를 위해 실행 중인 프로그램을 재컴파일하거나 프로세스를 중단시킨 후 재실행하여야 하는 제한이 있어, 프로세스 중단 없이 수행되어야 하는 응용 프로그램에 적합하지 않음
해결방안	• 공유 라이브러리 형태로 제작된 메모리 랜덤화 모듈을 실행 중인 대상 프로그램에 인젝트하여, 인젝트된 메모리 랜덤화 모듈이 대상 프로그램에 의해 이용되는 공유 라이브러리를 임의의 새로운 위치로 주기적으로 복사 및 변경하여 메모리 주소를 랜덤화하도록 함
기술의 특징 및 우수성	• 메모리 랜덤화를 위해 재컴파일이나 프로세스 중단이 요구되지 않으므로, **프로세스 중단 없이 수행되어야 하는 응용 프로그램에 대한 메모리 공격을 방어**할 수 있음

□ 기술의 효과

○ 메모리 랜덤화를 위해 실행 중인 프로그램에 대한 재컴파일이나 프로세스 중단이 요구되지 않으므로, 프로세스 중단 없이 수행되어야 하는 응용 프로그램에 대한 메모리 공격을 방어할 수 있음

□ 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	메모리, 주소, 라이브러리, 랜덤화, 공격
영문키워드	memory, address, library, randomization, attack

□ 기술의 적용분야

○ 본 기술은 소프트웨어에 대한 메모리 공격을 방어하기 위한 기술에 적용 가능함

[표] 적용분야

정보 보안
메모리 공격 방어

□ 기술경쟁력

○ 공유 라이브러리 형태의 메모리 랜덤화 모듈을 프로그램에 인젝트하는 간이한 방식을 통해 재컴파일이나 프로세스 중단 없이 메모리 랜덤화를 실행할 수 있음

□ 기술실시에 따른 기업에서의 이점

○ 종래 메모리 랜덤화 기술에 비해 프로세스 중단 없이 수행되어야 하는 응용 프로그램에도 적용 가능하므로 시장 경쟁력 확보 가능

[표] 메모리 공격 방어 기술 분야의 SWOT 분석

강점(Strength)	약점(Weakness)
• 메모리 공격에 따른 피해 사례 증가에 따라 방어 기술에 대한 수요 증대 • 미션 크리티컬 애클리케이션에 적합한 메모리 공격 방어 기술 부족	• 핵심 원천기술 부족 • 전문 인력 부족 • 중소 기업 위주의 시장 구조
기회요인(Opportunity)	**위협요인(Threat)**
• 메모리 공격 기술 발전에 따른 보안 위협 증가 • 클라우드 환경 등에서 미션 크리티컬 애플리케이션에 대한 요구 증가	• 정보 보안 분야에 대한 국가 R&D 투자 미흡 • 국내 정보 보안 시장 협소

□ 특허현황

구분	발명의 명칭	출원번호 (출원일)	등록번호 (등록일)	출원국가
1	프로세스 중단 없는 메모리 랜덤화 방법 및 이를 수행하기 위한 컴퓨팅 장치	10-2018-0136355 (2018.11.08.)	10-1961818 (2019.03.19.)	한국