Team No.

TONGMYONG UNIVERSITY

전공연구형_Capstone Design 신청서

과제명	국문	해시함수를 이용한 코드 난독화 프로그램 개발					
	영문	Development of Code Obfuscation Program Using Hash Functions					
과제팀명		안약					
참여학과		정보보호학과	교과목명		DID 인증 기술 _Capstone Design		
지도교수		성명				소속(학과)	
		신 승 수				정보보호학과	
참여학생	구분	소속학과(전공)	학번	학년	성명	연락처	이메일
	팀장	정보보호학과	18학번	3	김 * 형	010-5436-****	wogud3426@naver.com
	팀원	정보보호학과	17학번	3	김 * 원	010-2385-****	kty110365@gmail.com
		정보보호학과	18학번	3	김 * 원	010-4043-****	ghkdth9753@naver.com
		정보보호학과	18학번	3	김 * 현	010-4852-****	poiuy01201@naver.com
수행기간		2022년 9월 ~ 2022년 12월					
유형선택		☐ 기업성장형 ☐ 사회기여형 ☐ 창업연계형					
구분 / 지원금액		■ 전공연구형	☐ 과제창출형_C유형 (예산 300,000원)				
			■ 학술연구형_D유형 (예산 200,000원)				

동명대학교 현장실습지원센터 규정에 의거, 캡스톤디자인 과제를 성실하게 수행하고자 본 과제 신청서를 제출합니다.

붙임 : 과제 제안서 1부

2022. 09. 16.

신청인(대표학생) : 김 * * (인)

과제지도교수 : 신 승 수 (인)

동명대학교 현장실습지원센터장 귀하

<별지 제4호 서식> (개정 2018.03.12.) (2019.09.20.) 전공연구형

Capstone Design 과제 제안서

1. 과제 선정 배경 및 과제 수행 목적

- 역공학이란 기계장치 또는 시스템의 기술적인 원리를 구조분석을 통해 발견하고 새로운 아이디어를 추가하는 일련의 과정임. 실제로 역공학으로 악성코드 분석, 프로그램 버그 수정 등의 역할을 함.
- 그러나 역공학을 악용한 소프트웨어 크랙 혹은 게임 핵 제작과 같은 저작권 침해 사례가 증가하는 추세임. 한국저작권보호원의 2022년 1분기 온라인 저작권 침해 분석 보고서에 따르면 전 분기에 비해 소프트웨어 저작권 침해 건수가 11.8% 증가한 것으로 나타남.
- 이로 인해 개발자 외 특정 사용자가 소스 코드를 이해하기 어렵게 하는 코드 난독화 과정이 추가되었으며 이는 직접적인 파일 실행 없이 어셈블리어 코드 또는 소스 코드만을 분석하여 프로그램의 작동 원리를 유추하는 역공학 기법 중 정적분석 방법을 어렵게 함. 예를 들어 변수 이름을 의미 없게 짓거나, 순환문을 재귀 함수로 바꾸는 등의 방법이 존재함.
- 하지만 코드 난독화는 정적분석을 지연시킬 수 있을 뿐 불가능하게 만드는 것은 아니기에 보다 효율적으로 소프트웨어를 보호하기 위한 난독화 기법이 필요함.
- 이에 대한 방법으로 해시함수를 통해 변수 이름의 해시값을 생성하고 기존 변수들의 이름을 해시값으로 치환한 후 띄어쓰기를 제거하여 정적분석으로부터 소프트웨어를 보호하기 위한 코드 난독화 프로그램을 개발하고자 함.

2. 과제 수행 방법

- 해시함수를 통한 코드 난독화 기법의 효율성을 검증하기 위해 정적분석을 합법적으로 사용할 수 있는 공개 소스를 사용할 계획임.
- 공개소스를 빌드하게 되면 .exe 확장자를 가지는 실행 파일이 생성됨. 빌드 과정에서 만들어진 실행 프로그램은 가독성이 매우 떨어지는 0, 1의 형태인 기계어로 되어있음.
- 따라서 사람이 직관적으로 프로그램의 행위를 분석할 수 있도록 기계어를 어셈블리어 코드로 바꾸는 기능 포함하는 디스어셈블러와 디컴파일을 통해 작성된 언어의 소스 코드를 제공하는 디컴파일러를 선정함.
- 그리고 기본적인 정적분석 방법과 난독화 기법 등 선행되어야 할 학습을(PE Header, String, Resource, register 등) 마친 후 실행 프로그램에 관한 분석을 진행함.
- 정적분석 방법

  (1) 파일 스캐너 (ex. PEID)를 이용해 PE Header를 확인하여 파일의 컴파일 된 시기

와 메모리에 올라가는 Offset 주소 등을 확인함.

(2) Strings 또는 Resource Hacker 등을 이용해 파일에 대한 정보를 획득할 수 있다. 예를 들어 개발자가 넣어 놓은 에러 메시지, 디버깅용 메시지 그리고 프로그램 버전 정보 등이 이에 해당함.

(3) 디스어셈블러를 통해 .exe 파일에 대한 기계어를 어셈블리코드로 변환하고 디컴파일러를 이용해 파일의 소스 코드를 추출한다.

(4) 어셈블리코드와 파일의 소스코드를 통해 프로그램의 동작을 정적으로 분석함.

- 2015년 8월경 미국 국립 표준 연구소에서 표준으로 채택된 SHA-3 해시 함수를 이용해 프로그램에서 사용되는 모든 변수의 이름을 해시 값으로 변경하고 소스 코드에 작성되어 있는 공백 문자를 제거하는 프로그램을 구현하고 난독화를 진행함.
- 원본 프로그램과 코드 난독화를 진행한 프로그램의 정적분석 결과를 분석하여 난독화 프로그램을 이용한 코드 난독화가 정적분석을 대응하는데 효과가 있는지 확인함.

3. 결과물에 대한 기대효과 및 활용방안

- 해시 함수의 취약점이 발견되지 않으면 난독화된 변수들을 복호화하기 어려울 것으로 기대됨.
- 코드 난독화로 정적분석에 소요되는 시간을 증가시킴으로써 소프트웨어를 보호할 수 있을 것으로 예상됨.

- 4. 수행 일정

주요내용	추진일정													소요 기간(월)
	9월		10월				11월				12월			
자료조사 및 개념 학습	■	■												2주
디어셈블러, 디컴파일, 오픈소스 선정			■	■										1.5주
코드 난독화 프로그램 제작 및 테스트					■	■	■	■	■					4.5주
원본 파일, 난독화 된 파일 정적 분석										■	■	■		3주
분석 결과 비교 및 결론 도출												■	■	2주

5. 팀원별 역할

No.	성 명	담당 및 수행업무
1	김 * *	과제 발표, 일 분배 및 원본 파일 정적분석
2	김 * *	난독화 된 파일 정적분석 및 분석 결과지 작성
3	김 * *	분석 결과 도출 및 코드 난독화 프로그램 제작
4	김 * *	코드 난독화 프로그램 제작 및 테스트

<별지 제4호 서식> (개정 2018.03.12.) (2019.09.20.) **전공연구형**

6. 소요 예산

구분	용도 (과제수행과의 연관성)	품목	규격	단위	수량	단가	금액 (원)
회의비	과제 수행 팀원과의 회의 진행			주 1회 한정			(5000원 * 4)
합 계							200,000원