

2021년 전기 졸업과제 지도확인서

1. 졸업과제 내용

번 호	45	팀 명	서2재1조	분 과	D
과 제 명		커널 드라이버 개발을 통한 Crypto-Ransomware 탐지/차단 시스템 구현			
개 요		<p>Crypto-Ransomware의 작동을 Run-time에 차단하는 Monitoring System의 구현을 목표로 한다.</p> <ul style="list-style-type: none"> - 목표 System을 구현하기 위해 가상으로 조성된 분석 환경에서 샘플 랜섬웨어의 Payload에 대해 I/O trace를 기록하여 패턴화시킨 뒤 저장한다. - 알려지지 않은 프로세스의 File System에 대한 I/O trace를 자동으로 분석하고, Ransomware일 가능성이 높은 프로세스의 요청에 대해서 차단을 수행한다. 			

2. 구성원별 역할

학 번	이 름	구성원별 역할 (1인당 3줄 이상)
201524543	이재원	<ul style="list-style-type: none"> - 랜섬웨어 메커니즘 분석 및 패턴화 - 탐지 모니터 구현 - Github 저장소 관리 - 보고서 작성 및 발표
201524481	서희재	<ul style="list-style-type: none"> - 샘플 랜섬웨어 수집 - 랜섬웨어 분석용 가상환경 생성 - 차단 시스템 구현

상기와 같이 졸업과제를 지도함을 확인합니다.

2021 년 05 월 14 일

지도교수 권동환 (인)