2022-2학기 DU-도전학기 참가신청서

■ 신청 내용

과제명	주요기반시설의 IoT 취약점 분석 및 보안 솔루션 개발				
신청 유형	□ 개인 ■ 팀(팀명: DU-SeloT)				
도전 영역	■ 전공(주전공 또는 복수전공) □ 일반선택				
신청 학점	3학점				
신청자	성명	소속	학번	휴대전화	전공영역 선택
	김	컴퓨터공학과		010.	주전공
	박	컴퓨터공학과		010.	주전공
	이	컴퓨터공학과		010.	주전공
	조	컴퓨터공학과		010.	주전공

■ 소속 학과장 확인[전공영역 신청자만 해당]

도전학기 과제 내용을 확인하고 해당 과제를 학생 소속 학부(과)·전공학점으로 인정 받는 것에 동의합니다.

학생 성명	소속 학과장 확인			
김	(소속)	컴퓨터공학과	(성명)	(서명 또는 날인)
박	(소속)	컴퓨터공학과	(성명)	(서명 또는 날인)
이	(소속)	컴퓨터공학과	(성명)	(서명 또는 날인)
조	(소속)	컴퓨터공학과	(성명)	(서명 또는 날인)

■ 활동 서약 및 개인정보 수집/활용 동의

1. 도전학기 활동기간 동안 도전 과제를 성실히 수행할 것을 약속하며, 과제 수행 중 휴학 또는 자퇴할 경우 활동 지원비 전액을 반환하겠습니다.

2. 교내 프로그램 및 타 국고사업과 동일 또는 유사한 과제로 중복 지원 받지 않을 것을 약속하며, 이를 위반할 경우 DU-도전학기 이수 학점 취소 및 활동 지원비 전액을 반환하겠습니다.

3. 도전학기 참여와 관련한 개인 정보(성명, 소속, 학번, 연락처, e-mail, 활동 내용, 결과물, 수기 등)를 국고 사업 및 각종 평가 실적, 학교 홍보 등의 자료로 활용하는 것에 동의합니다.

2022년 08월 05일

(신청자 성명) 김 (서명 또는 날인)	(신청자 성명) 박 (서명 또는 날인)	(신청자 성명) 이 (서명 또는 날인)	(신청자 성명) 조 (서명 또는 날인)

2022-2학기 DU-도전학기 계획서

<table>
<tr><td>과제명</td><td colspan="4">주요기반시설의 IoT 취약점 분석 및 보안 솔루션 개발</td></tr>
<tr><td>신청 유형</td><td colspan="4">☐ 개인 ■ 팀(팀명: DU-SeloT)</td></tr>
<tr><td>도전 영역</td><td colspan="4">■ 전공(주전공 또는 복수전공) ☐ 일반선택</td></tr>
<tr><td>신청 학점</td><td colspan="4">3학점</td></tr>
<tr><td rowspan="5">참여자</td><td>성명</td><td>소속</td><td>학번</td><td>비고</td></tr>
<tr><td>조</td><td>컴퓨터공학과</td><td></td><td>팀장</td></tr>
<tr><td>김</td><td>컴퓨터공학과</td><td></td><td>팀원</td></tr>
<tr><td>박</td><td>컴퓨터공학과</td><td></td><td>팀원</td></tr>
<tr><td>이</td><td>컴퓨터공학과</td><td></td><td>팀원</td></tr>
<tr><td>지도교수 의견</td><td colspan="4">학생들이 도전하는 프로젝트는 현재 사이버보안 분야에서 가장 중요성이 높은 <주요기반시설 보안>에 해당되는 주제입니다. <주요기반시설 보안>을 위해서는 <클라우드 컴퓨팅>, <사물 인터넷>, <사이버보안> 등에 대한 전반적인 지식 및 경험이 필요합니다. 도전 학기에 참여하는 학생들은 컴퓨터공학전공의 <클라우드 컴퓨팅>, <정보보호>, <사물 인터넷>, <네트워크> 등의 교과목을 수강하여 기초 지식을 습득한 상태이고, 국가보안기술연구소 및 한국연구재단의 클라우드 보안 연구 프로젝트에도 참여하여 학술 논문을 다수 발표한 경력이 있습니다.
따라서 도전 학기 프로젝트의 목표를 충분히 달성할 수 있는 실력을 가지고 있다고 생각하고, 성공적인 프로젝트 완수를 위해 지도교수로서 적극 지원하겠습니다.

(소속) 컴퓨터공학과 (성명) (서명 또는 날인)</td></tr>
</table>

1. 도전 배경

주요 기반시설(Critical Infrastructure)은 외부 공격으로 인해 점령, 파괴 또는 기능이 마비될 시 국가 경제와 안보에 큰 영향을 미치는 중요한 시설이다. 이러한 주요 기반시설을 목적으로 하는 악의적인 사이버 공격의 횟수가 증가하고 있다. 최근 발생하는 사이버 공격의 경우 기존의 공격 탐지방식으로는 탐지하는 데 있어 어려움이 존재한다. 본 팀은 같은 학술 동아리에서 주요 기반시설 보안이라는 공통된 주제로 공부를 하던 중 도전 학기 프로그램을 알게 되어 직접 주요 기반시설을 구축해보며 공격이 발생할 수 있는 취약점을 조사하고 나아가 공격을 탐지하는 솔루션 개발을 도전해보려고 한다.

2. 도전 과제의 목표

가. 팀 목표 : 주요 기반시설(Critical Infrastructure)에는 도로, 항만, 국방 등 다양한 분야가 포함되어 있다. 과거 주요 기반시설은 내부망을 사용하여 외부의 공격에 노출되는 경우가 적었지만, 최근 클라우드 같은 기술의 도입으로 내부망에서 외부망으로 시스템을 옮겨 운영하게 되었다. 이와 같은 상황은 외부의 악의적인 공격에 노출될 수 있으므로 주요 기반시설에 대한 보안은 더욱 중요해질 것이다. 본 팀

은 주요 기반시설 중 도로 및 교통을 직접 구현해 보고 구현한 환경에서 발생할 수 있는 취약점 및 공격 데이터 수집을 진행한다. 나아가 수집한 공격 데이터를 기반으로 공격을 효율적으로 탐지할 수 있는 솔루션을 개발해보려고 한다.

나. 개인 목표

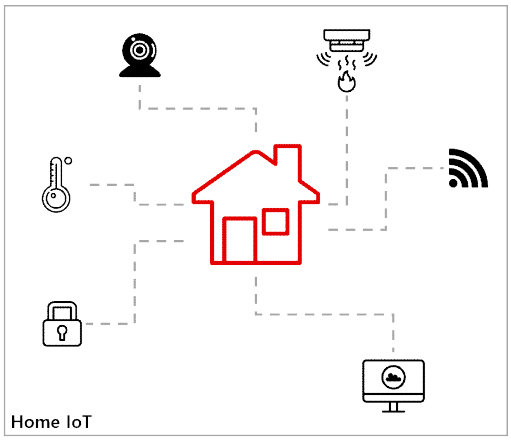
1) 자율 주행 자동차 개발을 통한 프로그래밍 역량 강화 및 IoT 보안 역량 강화(김태협)
   - 실제로 신호를 탐지하며 스스로 거리의 상황에 따라 움직이는 자율 주행 자동차의 개발을 진행하며, 동시에 인공지능 자동차 및 다양한 IoT 기기에서 발생할 수 있는 공격을 조사한다.
   - 가정에서 사용하는 다양한 IoT 기기의 조사 및 취약점 탐지 및 분석을 진행한다.
   - 인공지능을 개발하며 취약점 탐지를 통한 전공 역량 강화
2) 도로 교통 시스템 및 데이터베이스 구축을 통한 프로그래밍 역량 강화 및 IoT 보안 역량 강화(박재민)
   - 도로 위에 존재하는 신호등, 감시 카메라와 같은 기기들의 구현과 동시에 데이터베이스, 웹 서버를 구축하여 데이터 수집을 진행한다. 또한, 다양한 기기들의 취약점을 조사한다.
   - 가정에서 사용하는 다양한 IoT 기기의 조사 및 취약점 탐지 및 분석을 진행한다.
   - 도로 교통 시스템을 개발하며 취약점 탐지를 통한 전공 역량 강화하고자 함
3) 자율 주행 자동차 개발을 통한 프로그래밍 역량 강화 및 IoT 보안 역량 강화(이현우)
   - 실제로 신호를 탐지하며 스스로 거리의 상황에 따라 움직이는 인공지능 자동차의 개발을 진행하며, 동시에 인공지능 자동차에서 발생할 수 있는 IoT 공격을 조사한다.
   - 가정에서 사용하는 다양한 IoT 기기의 조사 및 취약점 탐지 및 분석을 진행한다.
   - 인공지능을 개발하며 취약점 탐지를 통한 전공 역량 강화
4) IoT에 발생할 수 있는 공격 주입 및 탐지를 통한 IoT 보안 역량 강화(조재한)
   - 도로 및 교통 환경에서 사용되고 있는 IoT 기기의 취약점을 분석하며 취약점을 사용해 발생하는 공격을 조사한다. 나아가 가정 내에서 사용되고 있는 다양한 IoT 기기의 취약점을 찾아본다.
   - IoT 기기의 취약점 분석 및 공격 탐지를 통한 전공 역량을 강화하고자 함

3. 도전 과제 내용

악의적인 공격이 발생하면 국가에 큰 피해를 줄 수 있는 주요 기반시설에 대한 보안은 매우 중요하다. 주요 기반시설에는 도로, 교통, 항만, 국방, 기지국, 발전소 등 매우 다양한 시설이 포함되어 있다. 이러한 주요 기반시설에 대한 외부의 공격은 꾸준히 발생하고 있으며 매년 발생 빈도가 증가하고 있다. 이러한 주요 기반시설은 과거 내부망을 통해 서비스를 운영하였다. 하지만 클라우드와 같은 기술의 발전으로 인하여 내부망에서 외부망으로 옮겨가며 악의적인 공격에 노출될 가능성이 과거에 비교해 높아졌다. 본 팀은 다양한 주요 기반시설 중 도로 및 교통 환경에서 존재하는 취약점을 조사하기 위해 직접 도로 및 교통 환경을 구축하여 취약점을 조사한다. 추가로 가정 내에서 사용하고 있는 IoT 기기들의 취약점을 조사해보며 수집한 공격 데이터를 기반으로 다양한 공격을 효율적으로 탐지할 수 있는 공격 탐지 솔루션을 개발하고자 한다.

가. 가정에서 사용하는 IoT 기기 취약점 조사

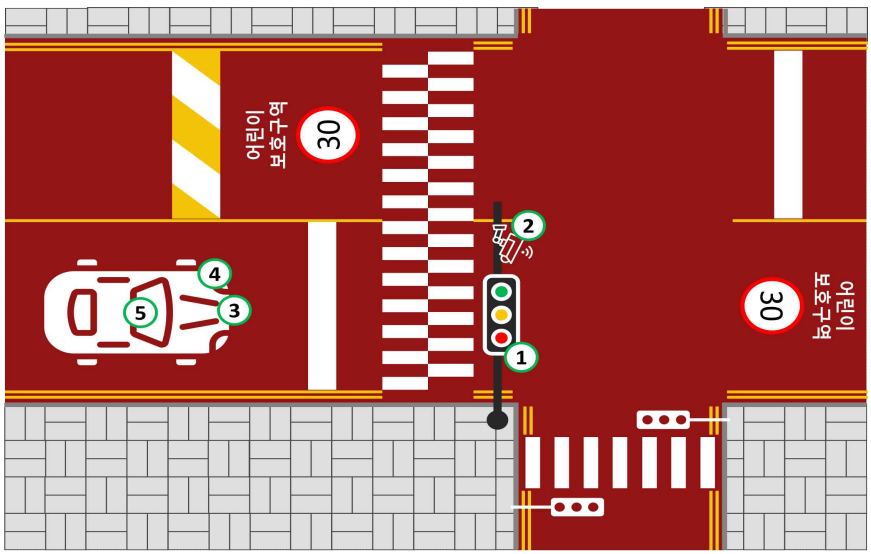
사물 인터넷 기술이 발전함에 따라 가정 내에서 편리성, 보안 등을 목적으로 다양한 IoT 기기들을 사용하고 있다. 대표적인 예로는 IP 카메라, 월 패드, 경보 센서 등이 있다. 네트워크에 연결되어 서비스를 제공하는 IoT는 이를 목적으로 하는 악의적인 공격의 빈도수가 꾸준히 증가하고 있다. 본 팀은 가정 내에서 사용하고 있는 IoT 기기의 취약점을 조사해보며 취약점을 사용해 발생할 수 있는 공격에 대해서 조사해 본다.



[그림 1] Home IoT 구조

나. 도로 및 교통 환경 구현, IoT 취약점 조사

1) 신호등 취약점 (도로)
 · 공격으로 인하여 정해진 신호가 아닌 신호로 변경되어 발생하는 시나리오를 구현함
2) 감시 카메라 취약점 (도로)
 · 공격으로 인하여 교통 법규를 지키고 있는 차량을 찍는 사고가 발생하는 시나리오를 구현함
3) 정지선 취약점 (도로)
 · 자율 주행 자동차가 공격으로 인하여 정지선을 인지하지 못하고 사고가 발생하는 시나리오를 구현함
4) 거리 센서 취약점 (교통)
 · IoT 공격으로 인하여 앞에 장애물이나 사람이 서 있는 경우 인지를 하지 못하여 자동차가 멈추지 못하여 사고가 발생할 수 있는 시나리오를 구현함
5) 웹 캠 취약점 (교통)
 · IoT 공격으로 인하여 신호등 인식, 사물 및 사람 인식을 방해하여 사고가 발생하는 시나리오를 구현함



[그림 2] 구현할 도로 및 교통 환경 도면

본 팀은 가정에서 사용하는 IoT 기기에 대한 취약점과 도로 및 교통에서 조사한 취약점을 통해 직접 공격을 주입하여 공격 데이터를 수집한다. 수집한 공격 데이터를 기반으로 기존의 공격 탐지 기법보다 효율적으로 공격을 탐지하는 공격 탐지 솔루션을 개발해보려 한다.

다. 업무분장 내용

팀원 성명	소속	담당 업무
김	컴퓨터공학과	- 자율 주행 자동차 개발 - 자율 주행을 위해 필요한 코드 작성 - 자율 주행 자동차 학습 - IoT 취약점 조사
박	컴퓨터공학과	- 도로 및 교통에 사용되는 기기 구현 - 구현한 다양한 기기의 데이터 수집 - 데이터 관리를 위한 데이터베이스 개발 및 웹 서버 구축
이	컴퓨터공학과	- 자율 주행 자동차 개발 - 자율 주행을 위해 필요한 코드 작성 - 자율 주행 자동차 학습 - IoT 취약점 조사
조	컴퓨터공학과	- 도로 환경 구축 - IoT 기기에서 발생할 수 있는 공격 조사 및 공격 주입 - IoT 취약점 조사

4. 도전 과제 추진일정

주차	활동 목표	활동 내용	투입 시간
1주차	실험 환경 구축 및 공격 시나리오 제작	조(팀장) : 도로 및 교통 환경 제작	9시간
		김(팀원) : 자율 주행 자동차 제작	8시간
		박(팀원) : 데이터베이스 설계	10시간
		이(팀원) : 자율 주행 자동차 제작	8시간
2주차	실험 환경 구축 및 공격 시나리오 제작	조(팀장) : 도로 및 교통 환경 제작	8시간
		김(팀원) : 자율 주행 자동차 코딩 작업	10시간
		박(팀원) : 데이터베이스 설계	8시간
		이(팀원) : 자율 주행 자동차 코딩 작업	10시간
3주차	실험 환경 구축 및 공격 시나리오 제작	조(팀장) : 도로 및 교통 환경 제작	8시간
		김(팀원) : 자율 주행 자동차 코딩 작업	10시간
		박(팀원) : 웹 서버 구축	8시간
		이(팀원) : 자율 주행 자동차 코딩 작업	10시간
4주차	실험 환경 구축 및 공격 시나리오 제작	조(팀장) : IoT 공격 조사	6시간
		김(팀원) : 자율 주행 자동차 학습	6시간
		박(팀원) : 웹 서버 구축	6시간
		이(팀원) : 자율 주행 자동차 학습	6시간
5주차	구축 환경 테스트 및 공격 조사	조(팀장) : IoT 공격 조사	6시간
		김(팀원) : 구축 환경 테스트	5시간
		박(팀원) : 구축 환경 테스트	5시간
		이(팀원) : 구축 환경 테스트	5시간
6주차	구축 환경 테스트 및 공격 조사	조(팀장) : IoT 공격 조사	5시간
		김(팀원) : IoT 공격 Tool 조사	4시간
		박(팀원) : IoT 공격 조사	5시간
		이(팀원) : IoT 공격 Tool 조사	4시간
7주차	구축 환경 테스트 및 공격 조사	조(팀장) : IoT 공격 조사	5시간
		김(팀원) : IoT 공격 Tool 조사	5시간
		박(팀원) : IoT 공격 조사	5시간
		이(팀원) : IoT 공격 Tool 조사	5시간
8주차	중간 보고서 작성	조(팀장) : 중간 보고서 작성	5시간
		김(팀원) : 중간 보고서 작성	5시간
		박(팀원) : 중간 보고서 작성	5시간

		이(팀원) : 중간 보고서 작성	5시간
9주차	공격 주입 및 공격 데이터 수집	조(팀장) : 공격 데이터 수집 및 분석	6시간
		김(팀원) : 구축한 환경에 공격 주입	6시간
		박(팀원) : 공격 데이터 수집 및 분석	6시간
		이(팀원) : 구축한 환경에 공격 주입	6시간
10주차	공격 주입 및 공격 데이터 수집	조(팀장) : 공격 데이터 수집 및 분석	6시간
		김(팀원) : 구축한 환경에 공격 주입	6시간
		박(팀원) : 공격 데이터 수집 및 분석	6시간
		이(팀원) : 구축한 환경에 공격 주입	6시간
11주차	공격 데이터 분석	조(팀장) : 공격 데이터 분석	5시간
		김(팀원) : 분석 데이터 그래프 작성	5시간
		박(팀원) : 공격 데이터 분석	5시간
		이(팀원) : 분석 데이터 그래프 작성	5시간
12주차	공격 데이터 분석 및 탐지 방법 연구	조(팀장) : 수집 데이터로 공격 방법 연구	5시간
		김(팀원) : 공격 데이터 분석	4시간
		박(팀원) : 수집 데이터로 공격 방법 연구	5시간
		이(팀원) : 공격 데이터 분석	4시간
13주차	공격 데이터 분석 및 탐지 방법 연구	조(팀장) : 공격 탐지 솔루션 개발	5시간
		김(팀원) : 수집 데이터로 공격 방법 연구	5시간
		박(팀원) : 공격 탐지 솔루션 개발	5시간
		이(팀원) : 수집 데이터로 공격 방법 연구	5시간
14주차	공격 데이터 분석 및 탐지 방법 연구	조(팀장) : 최종 데이터 정리	6시간
		김(팀원) : 공격 탐지 솔루션 개발	6시간
		박(팀원) : 공격 탐지 솔루션 개발	6시간
		이(팀원) : 공격 탐지 솔루션 개발	6시간
15주차	최종 보고서 작성	조(팀장) : 최종 보고서 작성	5시간
		김(팀원) : 최종 보고서 작성	5시간
		박(팀원) : 최종 보고서 작성	5시간
		이(팀원) : 최종 보고서 작성	5시간

5. 활동 지원비 상세 내역

활동 지원비 신청내역			
항 목		산출근거	금액(원)
재료비		- 「라즈베리 파이 4, 8GB」* 2세트 - 270,000원 * 2세트 = 540,000원 - 「아두이노 신호등 프레임 세트」* 3세트 - 33,000원 * 3세트 = 99,000원 - 도로 안전센서 키트 (모션, 초음파, 부저 등) - 15,000원 * 2세트 = 30,000원	669,000원
회의비		- 팀 회의비 - 7,000원 * 4명 * 15주	420,000원
등록비		- 한국 멀티미디어학회 추계학술대회 등록비 - 100,000원 * 4명 = 400,000원	400,000원
교통비	KTX	- 동대구 - 서울 왕복 KTX 기차비 - 87,000원(왕복) * 4명 * 1회 = 348,000원	348,000원
인쇄비	도로 환경 제작	- A1, 2장 분량, 교통 환경 제작 - A+ 인쇄소 기준 견적 가격	40,000원
	학술대회 포스터제작비	- A1, 2장 분량 - A+ 인쇄소 기준 견적 가격	40,000원
합계(원)			**1,917,000원**

6. 과제 수행 후 제출할 수 있는 결과물

도전 학기 활동은 수행하면서 제출할 수 있는 결과물로는 팀 공통 결과물이 있다. 팀 공통 결과물은 IoT 공격을 탐지할 수 있는 공격 탐지 프로그램과 수집한 공격 데이터를 기반으로 분석한 내용으로 학술대회 논문을 작성하려 한다. 도전 학기로 진행하는 프로젝트로 나오는 공격 탐지 프로그램은 팀원 모두가 참여하였으며 만드는 과정에 수집한 데이터 또한 팀원 전체가 수집하고 분석하였기 때문에 팀 공통 결과물로 공격 탐지 프로그램과 학술대회 논문을 제출하고자 한다.

가. 팀 공통 결과물 : 공격 탐지 프로그램 (Application)
학술대회 논문