


2024학년 1학기 노트북(Macbook) 활용보고서

제출자			
이름(학번)	이진주	제출일	20240210
맥북 관리번호	2019-B002	연장/반납여부	연장
현재 맥북 및 부속품사진(관리번호가 선명히 나오게)			
맥북(앞면)		맥북(뒷면)	
			
맥북 (안쪽면-디스플레이화면부터 키보드자판까지 모두)		부속품 (충전기-전원 어댑터, 케이블)	
			

□ 활용결과물

- 노트북을 활용한 내용(제목 당 1페이지이내작성)(개발결과물 URL 기재 / 소스코드 깃허브 URL 기재)

제목	PushPush multiplayer game
수행기간	2024.12월 말 - 1월 중순
활용 목표 및 내용	<p>네트워킹을 활용한 채팅 프로그램을 base로 하여 멀티 유저간 플레이가 가능한 pushpush game을 만들어 보았다. 방학 중 캡스톤 스타디를 본격적으로 시작하기 전에 팀끼리 협업하여 어느 정도 규모가 있는 프로젝트를 개발하고 유지보수 해보는 경험을 익히기 위해서 주어진 과제였다. 1000 줄이 넘어가는 코드를 짜고 서로 코드 리뷰를 하며, github를 이용해 버전관리, merge와 pull request, issue tracking 등을 연습해볼 수 있었다.</p> <p>게임은 퓨어 C로 개발되었으며 GUI를 붙이기 위하여 GTK 라이브러리를 간단하게 공부하여 사용하였다. TCP 네트워킹을 통해 서버와 클라이언트가 소통하는 방식을 사용하였으며, MVC모델에 기반하여 모델 설계와 프로토콜을 미리 토의한 후 시작하였고, 게임 데이터(맵, 유저의 base위치, item의 정보 등)는 서버에 json 형태의 input을 넣어 주어 로딩하는 방식을 채택하였다. 서버는 controller를 echo하는 역할을 수행하고 클라이언트 단에서 대부분의 게임 로직을 처리하도록 개발하였다.</p>
수행결과	<p>다음과 같은 GUI가 제공된다.</p>  <p>키보드의 상하좌우 key를 사용해 캐릭터를 움직일 수 있다. 장애물은 밀거나 통과할 수 없다. 몸으로 item을 밀어 자신의 base에 넣으면 score가 증가한다. Map 안의 모든 item이 소진되거나 미리 설정된 timeout 시간에 도달하면 게임이 종료된다.</p> <p>Github url: https://github.com/leejjju/capston-PushPush.git</p>

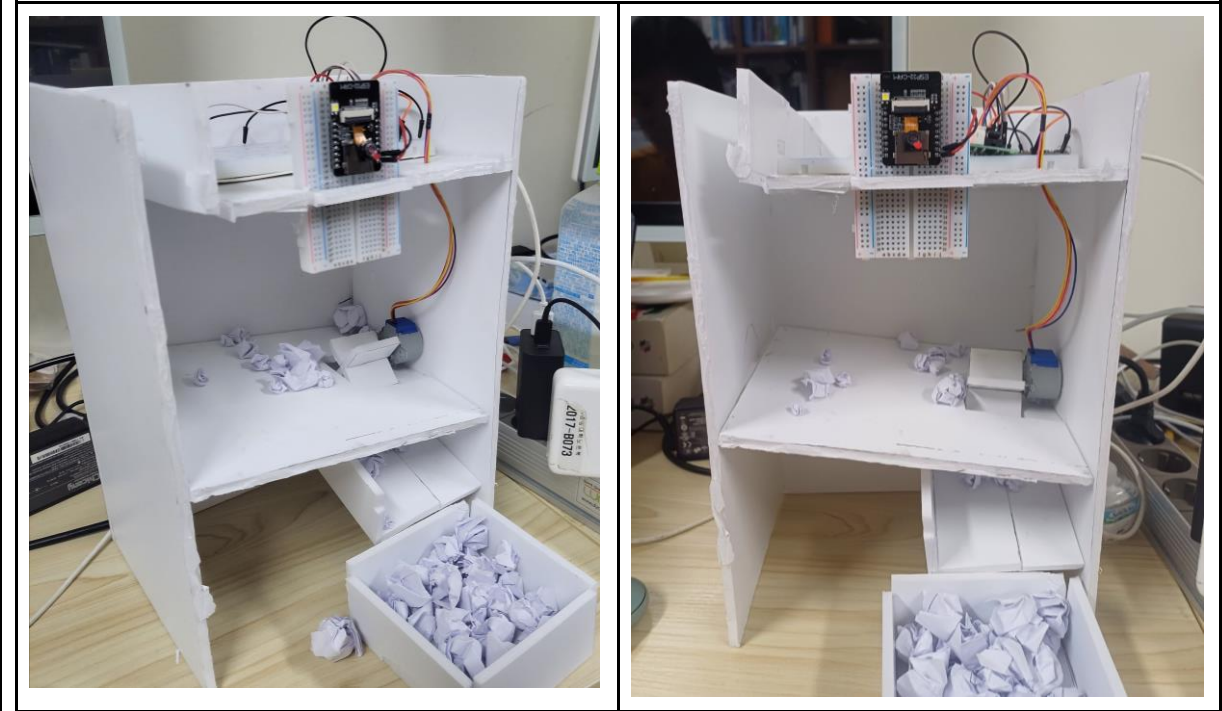
□ 활용결과물

- 노트북을 활용한 내용(제목 당 1페이지이내작성) (개발결과물 URL 기재 / 소스코드 깃허브 URL 기재)

제목	IoT설계과제: 애완동물자동급여기
수행기간	2023.11월 말- 12월 초
활용 목표 및 내용	<p>이번 학기 수강한 IoT시스템 설계 과목의 Final 설계 과제로 제출했던 프로젝트이다.</p> <p>애완 동물을 집에 두고 등교 혹은 출근을 해야 하는 사람들을 위하여 원격 제어가 가능한 자동 급여기를 제작하였다. 기능은 설정된 시간의 자동 급여, 원격 제어를 통한 자동 급여, 캠을 통해 애완동물의 모습 확인 및 라이트 제어, 급여시 소리를 발생시켜 애완 동물에게 급여 사실 알리기 등이다.</p> <p>라즈베리파이를 서버로 두는 Home assistant, NodeMCU와 mqtt 프로토콜을 사용하였다. Esp32-cam, passive buzzer, step motor 등을 사용하였으며 우드락과 글루건을 사용하여 blueprint의 설계를 따라 실제 급여기의 프로토타입 또한 제작해보았다. blueprint부터 설계, 코딩, 프로토타입 제작까지 하나의 흐름을 모두 경험해볼 수 있어 인상 깊은 프로젝트였다.</p>

수행결과

프로토타입

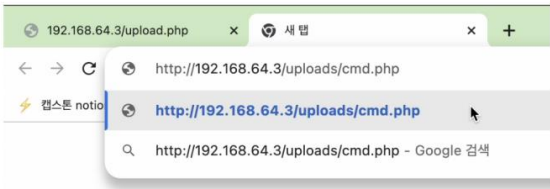



사용안내 README

<https://docs.google.com/document/d/1rW6y1hgr7MCPIGMRg6UZA4N3C7P9UsQLc914hRgkRCE/edit>

□ 활용결과물

- 노트북을 활용한 내용(제목 당 1페이지이내작성)(개발결과물 URL 기재 / 소스코드 깃허브 URL 기재)

제목	File upload 취약점을 활용한 Ransomware 공격 및 대응
수행기간	2023.11월 말 - 12월 초
활용 목표 및 내용	<p>이번 학기 수강한 컴퓨터 보안 과목의 Final 프로젝트로 제출했던 과제이다.</p> <p>주제는 file upload attack과 ransomware를 결합하여 하나의 공격 시나리오를 보여주고 그를 예방하는 코딩 스타일을 구현하는 것으로 하였다.</p> <p>직접 취약점을 가진 웹 서버를 간단히 만들어 file upload 기능을 구현하고, 간단한 웹 쉘을 업로드하여 권한을 탈취할 수 있도록 하였다. 또한 단순한 웹 쉘로는 권한이 제한되기에, 좀 더 직접적인 공격을 위해 keylogger를 사용하였으며, 그를 통해 ransomware가 실행되는 과정까지 재현해 보았다.</p> <p>그리고 시나리오의 근본적 원인인 file upload attack을 막기 위해 file upload 기능을 코딩할 때 지켜야 할 주의 사항을 찾아보고 직접 적용해 시나리오가 막히는 모습을 확인하였다.</p>
수행결과	<div>  <p>그림 2. 파일 업로드 폼더 경로 확인</p> <p>시스템 관리자가 만약 시스템 명령어 및 관리자 비밀번호를 입력한 기록이 있다면 Keylogger 파일에 기록되고 있을 것이다. 웹 쉘을 통해 Keylogger 파일을 업로드하여 관리자의 비밀번호를 탈취한다.</p> <pre> Enter a Command: cat /var/log/logkeys.log Output: cat logkeys/build/testlog.log Key Logger: cat /var/log/logkeys.log cat ./jpe cmd.php cat ../index.html </pre> <p>그림 3. Keylogger 파일</p> <pre> 2023-12-06 21:54:43+0000 > zu yon 2023-12-06 21:54:46+0000 > K 2023-12-06 21:54:57+0000 > zu uc 2023-12-06 21:54:59+0000 > KJ 2023-12-06 21:55:04+0000 > .tau 21800213 </pre> </div> <div> <p>탈취한 비밀번호로 ssh를 통해 관리자 계정으로 로그인 하여, sudo 권한으로 랜섬웨어 파일을 실행시켜 모든 파일을 암호화한다.</p> <pre> (base) naborim@nabolim-ui-MacBookPro-2 ~ % ssh naborim@192.168.64.3 naborim@192.168.64.3's password: </pre> <p>그림 5. 탈취한 관리자 비밀번호로 ssh를 통한 접속</p>  <p>그림 6. 랜섬웨어로 감염된 관리자 웹 사이트</p> <p>이와 같은 공격을 보완하기 위해서 파일의 확장자를 검증하여 이미지 업로드 웹사이트의 경우 이미지 확장자(jpeg, gif, png, jpg)의 파일만 업로드 할 수 있도록 설정하거나, 업로드 파일의 실행 권한을 제한하거나, 외부에서 파일을 식별할 때 파일명을 무작위로 지정하여 식별할 수 없도록 하는 방법 등을 통해 파일 업로드 공격으로부터 시스템을 방어하고 있다.</p> </div>

발표 자료: https://docs.google.com/presentation/d/15_S5xsw-H31AsEvpO-PTYqdh0bibac5-w5hF_SQFoU/edit#slide=id.p