



아두이노를 이용한 BadUSB 제작 프로젝트



중부대학교 SCP 정보보안 동아리
2022 동계 방학 프로젝트

1학년 부원 노무승

목 차

1. 개요

1-1. BadUSB란?

1-2. 아두이노란?

1-3. HID 기능

2. 계획

2-1. 아두이노 모델 선정

2-2. Malware Command

(Win 단축키 + PowerShell)

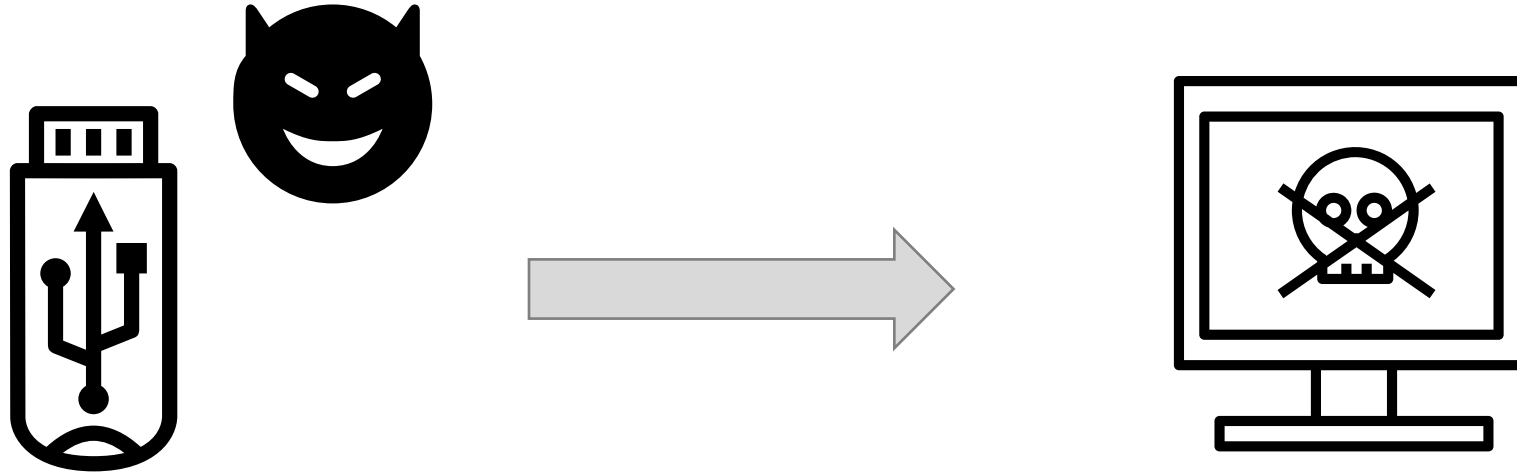
2-3. UAC Bypass

3. 활용



1. 개요

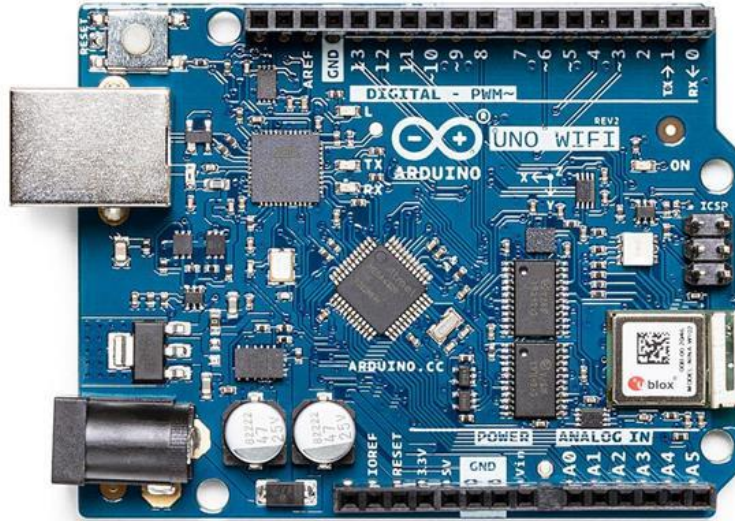
1-1. BadUSB란?



USB를 조작하여 해킹용 도구로 만들어 공격하는 기법.

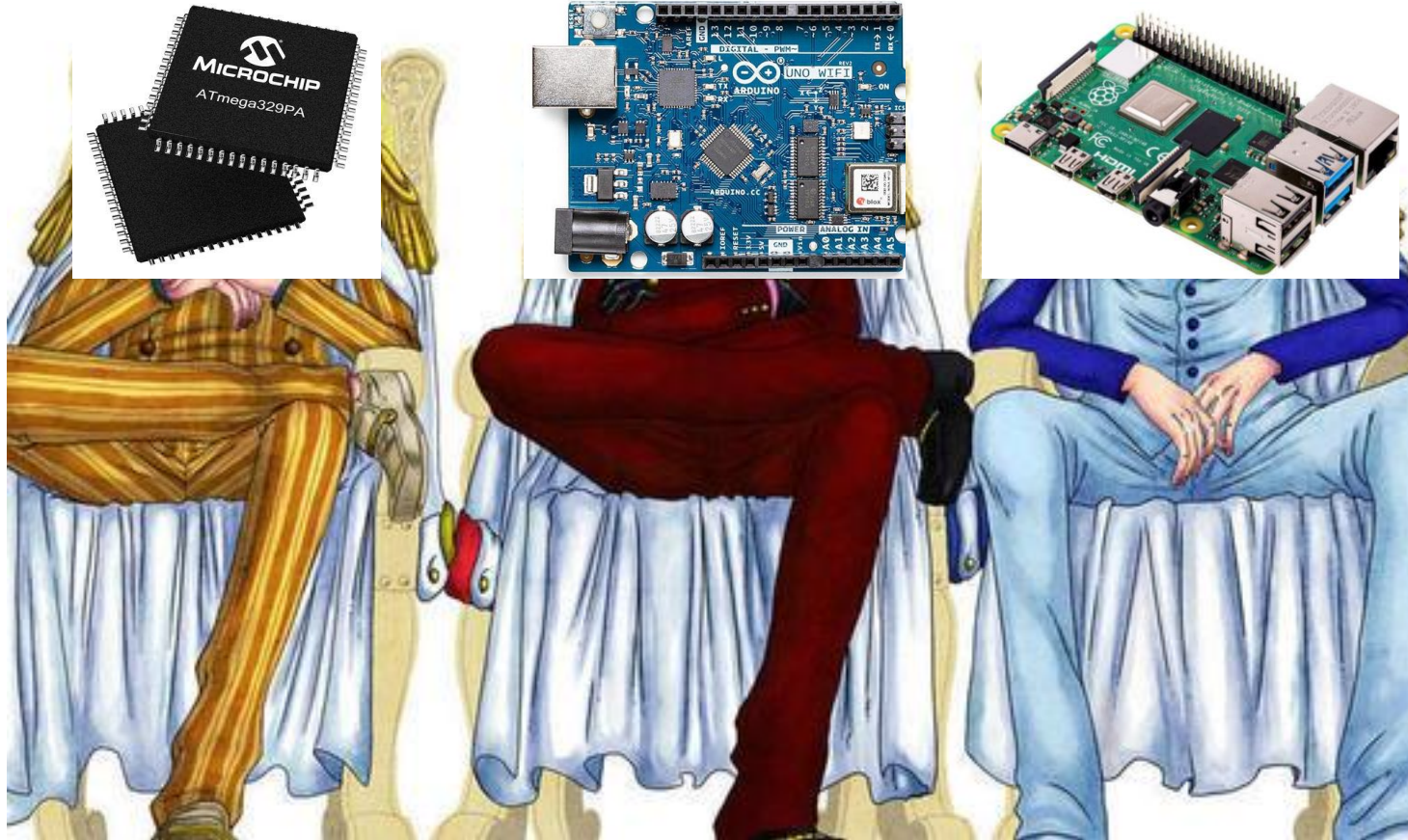
(펌웨어 조작, **HID**, USB Killer(?), ...)

1-2. 아두이노란?



‘마이크로컨트롤러’를 사용하여
Code 레벨에서 손쉽게 전자 부품을 제어, 프로그래밍 할 수 있는 도구

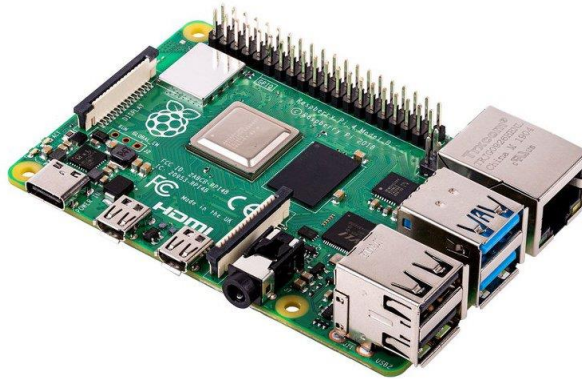
1-2. 아두이노란?



임베디드 프로그래밍 3대장.jpg

1-2. 아두이노란?

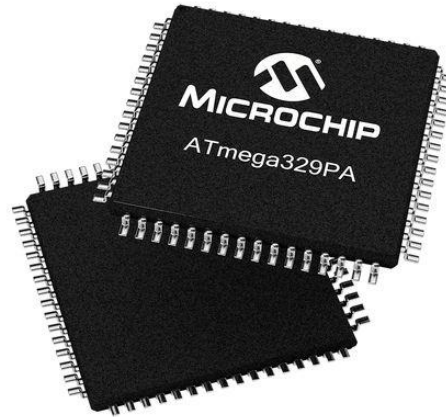
A. 라즈베리파이랑 비슷한거 아니가요?



Q. ㄴㄴ, 라즈베리파이는 '마이크로프로세서'를 사용하고,
OS가 올라가야 동작하기 때문에 아두이노랑 비교했을 때
가격 ↑, 전력 ↑, 발열 ↑, 번거로움 ↑, 버퍼링 ↑

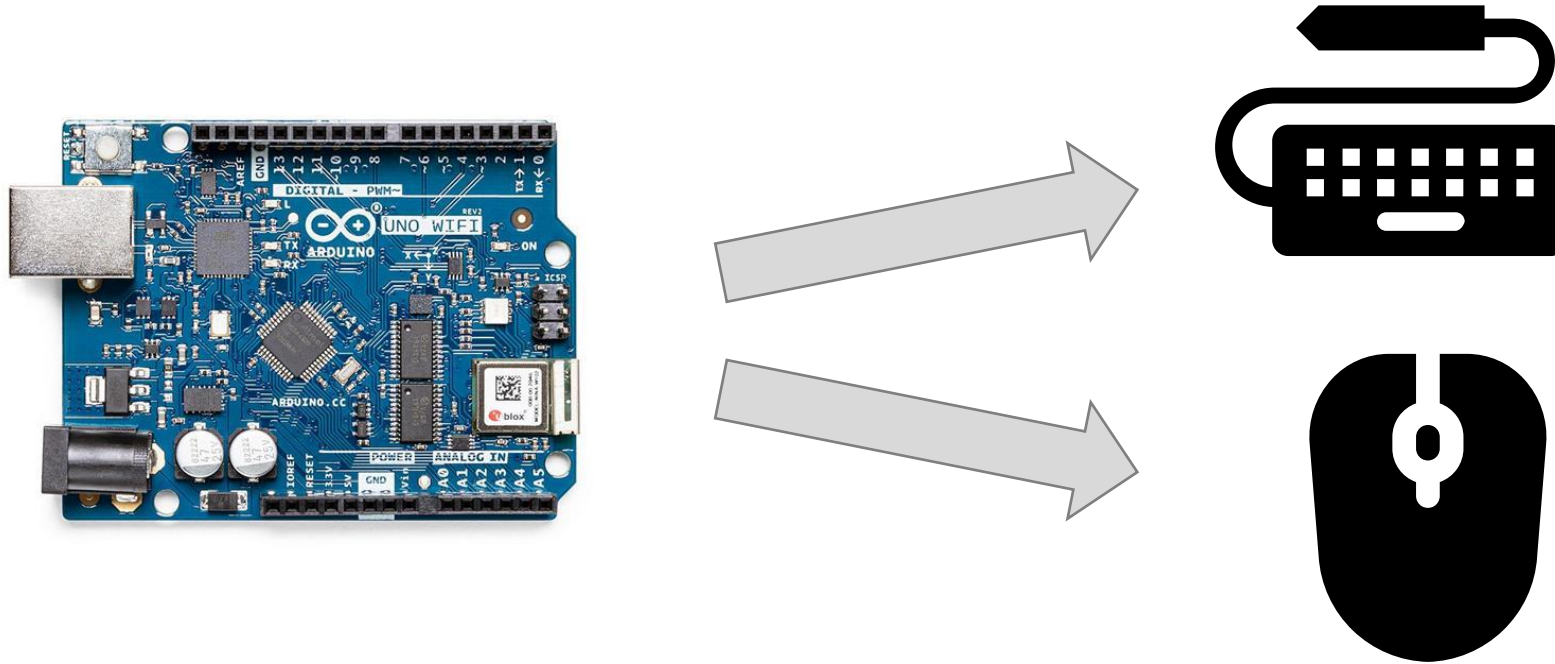
1-2. 아두이노란?

A. RAW레벨에서 접근하려면 AVR MCU에
바로 프로그래밍 하는게 좋지 않을까요?



Q. AVR이 RAW레벨에서 접근하기 용이하고
필요한 칩만 사용할 수 있는 것은 사실이지만
전기전자공학도가 아니기 때문에 일단 논외로 합니다

1-3. HID 기능



사용자 인터페이스 장치(Human interface device, HID)란
컴퓨터 주변 기기 중 사용자 인터페이스를 담당하는 것을 말한다.

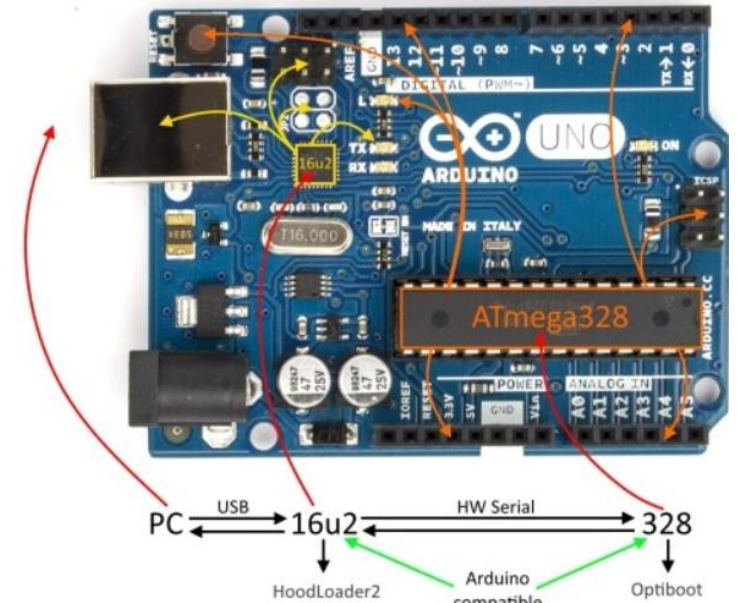
1-3. HID 기능



아두이노 프로 마이크로
(atmega32u4)



아두이노 레오나르도
(atmega32u4)



아두이노 우노, ...
(atmega16u4+328)



2. 계획

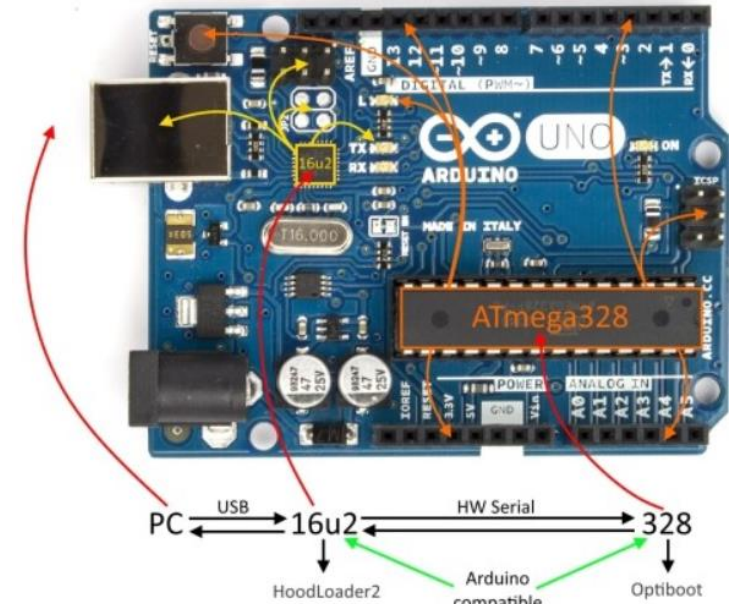
2-1. 아두이노 모델 선정



아두이노 프로 마이크로
(atmega32u4)

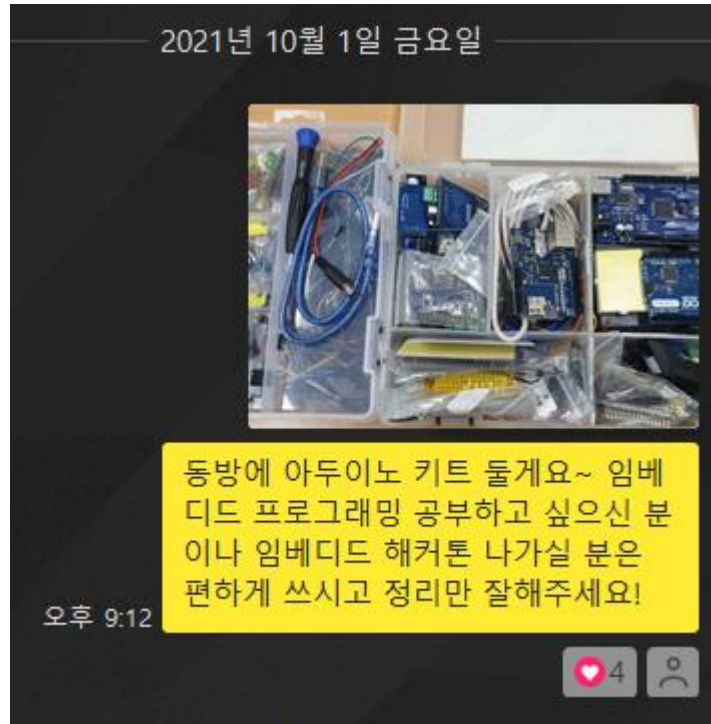


아두이노 레오나르도
(atmega32u4)



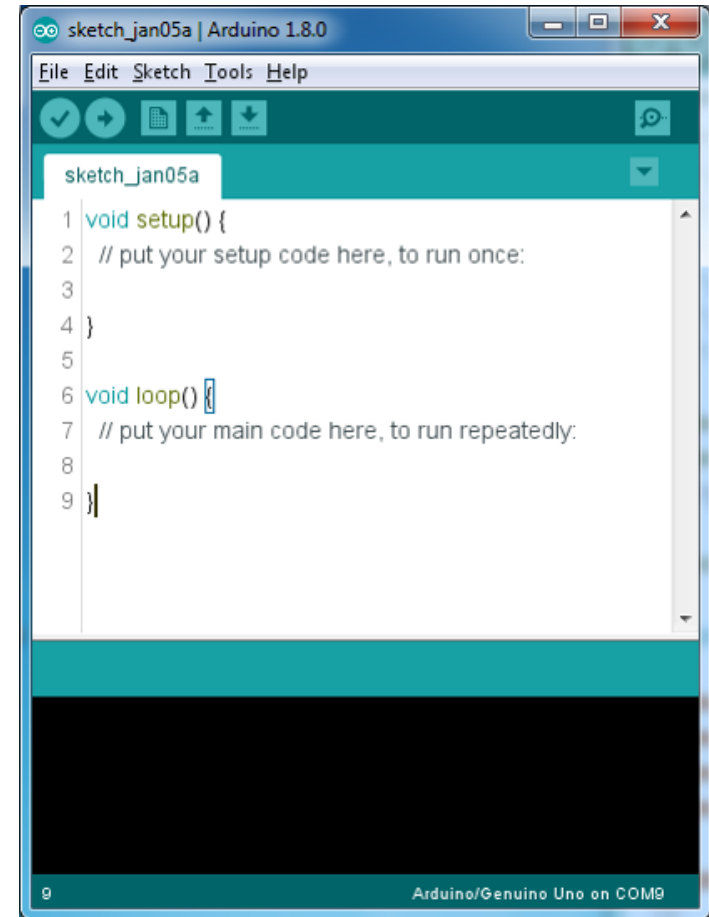
아두이노 우노, ...
(atmega16u4+328)

2-1. 아두이노 모델 선정

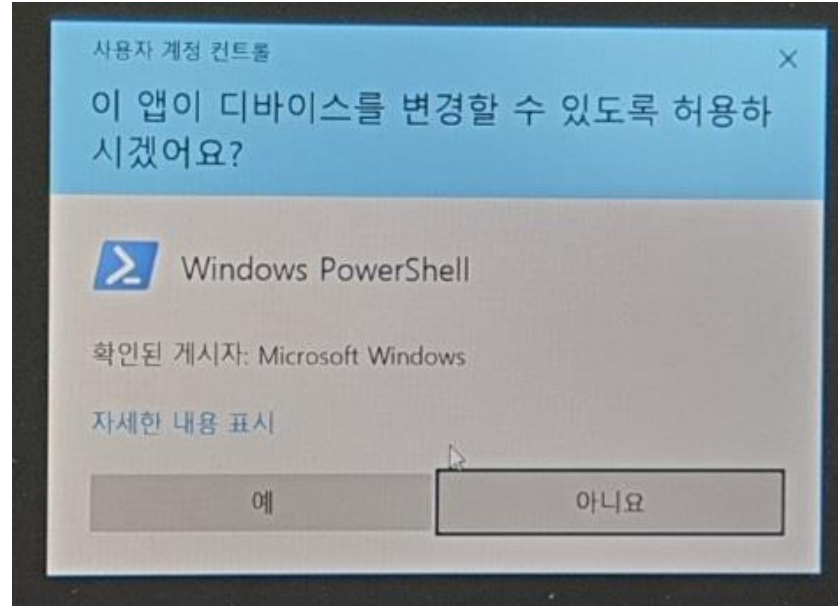


2-2. Malware Command

1. 윈도우 실행창 오픈
(Windows Key + R)
2. 0.5초 딜레이
3. 악성코드 다운 및 실행
(Powershell 명령어)



2-3. UAC Bypass

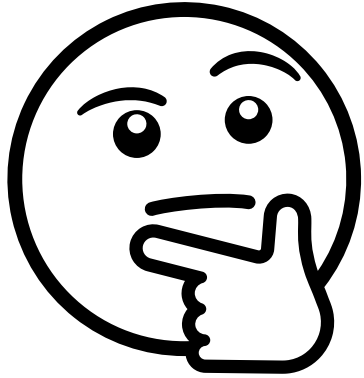


사용자 계정 컨트롤 (User Account Control, UAC) :

윈도우 Vista 이후부터 추가된 기능으로

관리자 권한을 얻기 위해서 사용자의 허락을 받게 하는 보안 정책.

2-3. UAC Bypass



나의 악성코드가 더 많은 기능을 수행하기 위해서는
UAC를 우회하여 관리자 권한을 취득하여야 함.



...

4. 0.5초 딜레이

5. UAC Bypass
(왼쪽 방향키+ 엔터)



3. 활용

3-1. 산출물 활용



BadUSB 관련 논문은 차고 넘쳐서 퀄리티는 떨어지지만
대비방안을 추가할 수 있다면 제출하는 것에 의의.



아두이노 코드 내용과 Malware Command 내용을
보완해서 10분~20분 정도로 대외 발표는 가능할듯.



Q & A





감사합니다

