IP 카메라 취약점 분석 및 네트워크 공격 자동화 도구 개발

팀　　명 : LS2K

팀　　원 : 이예준, 손경현, 송태현, 김수현

지도교수 : 진수현

00 Table of Contents

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

프로젝트 소개

- 팀 소개
- 프로젝트 주제 선정
- 프로젝트 개요

진행 과정

- 분석 대상 선정
- 펌웨어 추출
- 취약점 분석
- 취약점 검증 및 구현

프로젝트 결과

- 취약점 제보 (KVE)
- 자동화 도구 개발
- IoT 기기 분석 능력 ↑
- 향후 계획

Ⅰ. 프로젝트 소개

팀 소개

Project Mentor

진수현 교수

Project Manager (PM)

이예준

취약점 분석

Project Agent (PA)

김수현

취약점 분석

Project Agent (PA)

손경현

데이터 분석

Project Agent (PA)

송태현

데이터 분석

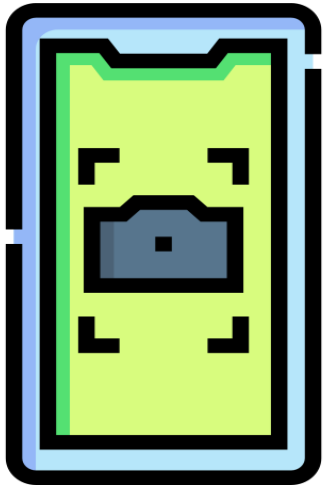
CCTV

기존의 사용하던 보안용 감시 카메라

유선으로 구성된 회로를 통해 구축되어 있으며, 설치된 구역 안에서만 영상 송출이 가능

프로젝트 주제 선정

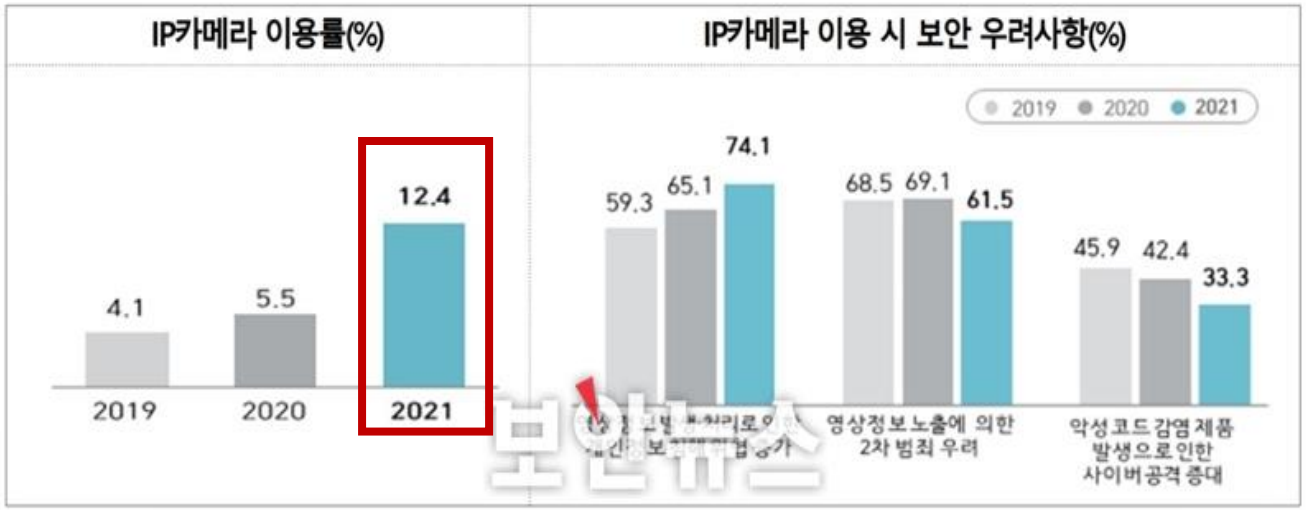
원격 제어 및 영상 확인 가능



IP Camera

컴퓨터 네트워크와 인터넷을 통해 데이터를 송수신 할 수 있는 카메라

프로젝트 주제 선정



<그림> IP카메라 이용률과 보안 우려사항 [자료=과기정통부]

프로젝트 주제 선정

가정집 IP카메라 해킹해 7092차례나 불법 촬영...20대 징역 4년

해킹 프로그램 이용 여성 신체나 성관계 모습까지
8차례 걸쳐 129만원 받고 제3자에게 유출도

(수원=뉴스1) 유재규 기자 | 2022-08-31 17:54 송고

https://www.news1.kr/articles/4789580

https://www.seoul.co.kr/news/newsView.php?id=20191017500111&wlog_tag3=naver

서울신문

IP카메라 1853대 해킹해 훔쳐봤는데 징역 1년

입력 : 2019-10-17 15:31 | 수정 : 2019-10-17 16:14

IP 카메라 해킹해 7000명 사생활 엿본 20대...징역 4년

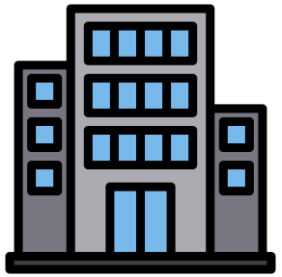
[illegible] IP 카메라 해킹
피해자 대부분 피해 사실 인지 못해
[illegible] 표적

입력 2022-08-31 18:29

https://m.kmib.co.kr/view.asp?arcid=0017426926

수년간 끊이지 않는 보안 사고, 피해자는 피해 사실을 인지 못함.

기존 보편적인 취약점 분석 방법론



기업 단위
취약점 분석 요청

White Box 환경
취약점 분석

취약점 검증
및 구현

* White Box Testing : 개발된 내부 소스코드를 보면서 취약점을 분석하는 방법

본 프로젝트의 취약점 분석 방법론

장비 수급 및
펌웨어 추출

Black Box 환경
취약점 분석

취약점 검증
및 구현

취약점 제보
보안 향상

* Black Box Testing : 소스코드와 내부 구조를 모르는 상태에서 취약점 분석을 진행

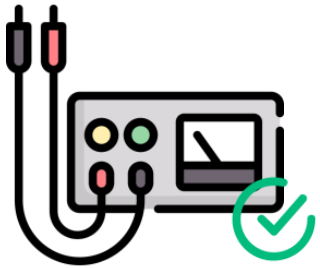
Ⅱ. 진행 과정

분석 대상 선정

장비 사진			
제조사	홈플래닛	티피링크	헤이홈
분류	IP 카메라	IP 카메라	IP 카메라
모델명	ZX-C24	Tapo C210	GKW-MC057A

Overveiw

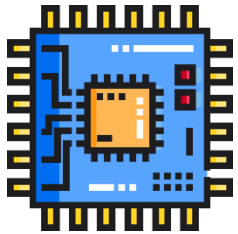
작동 테스트 및 분해



통전 테스트로
UART PIN 식별

UART Soldering

false

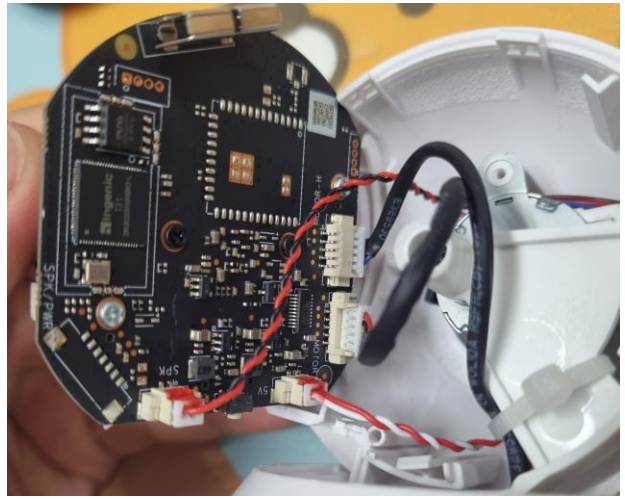


SPI 통신
펌웨어 추출

true

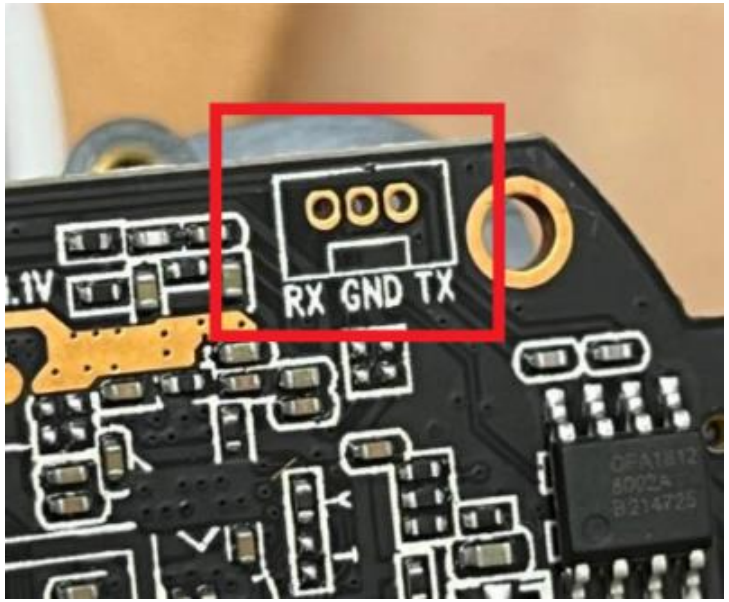
UART Shell 연결 후
펌웨어 추출

작동 테스트 및 분해

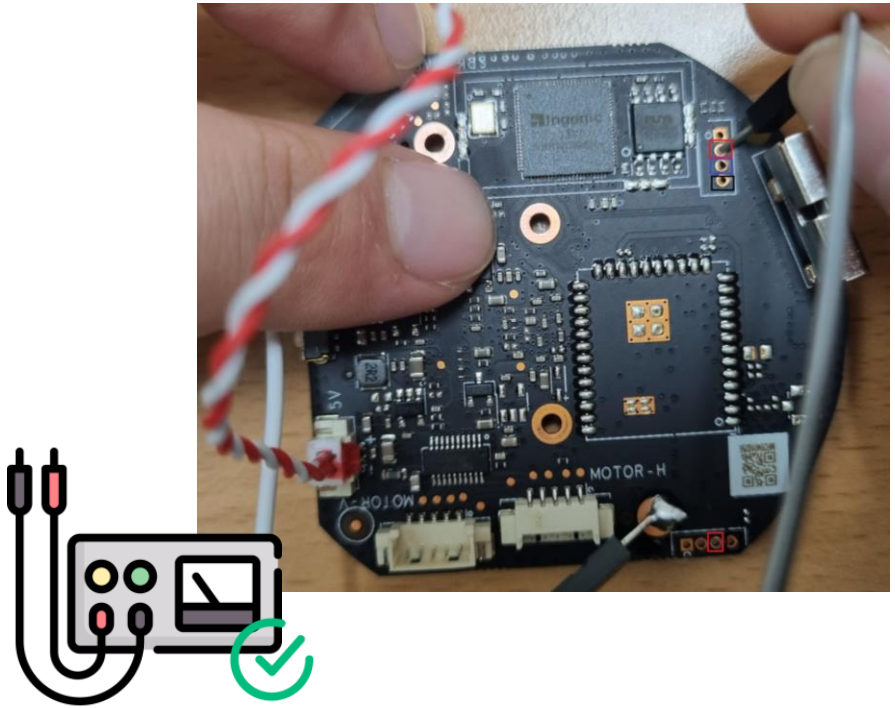


각 기기마다 정상작동 및 기능 확인 후 장비 분해

통전 테스트로 UART PIN 식별

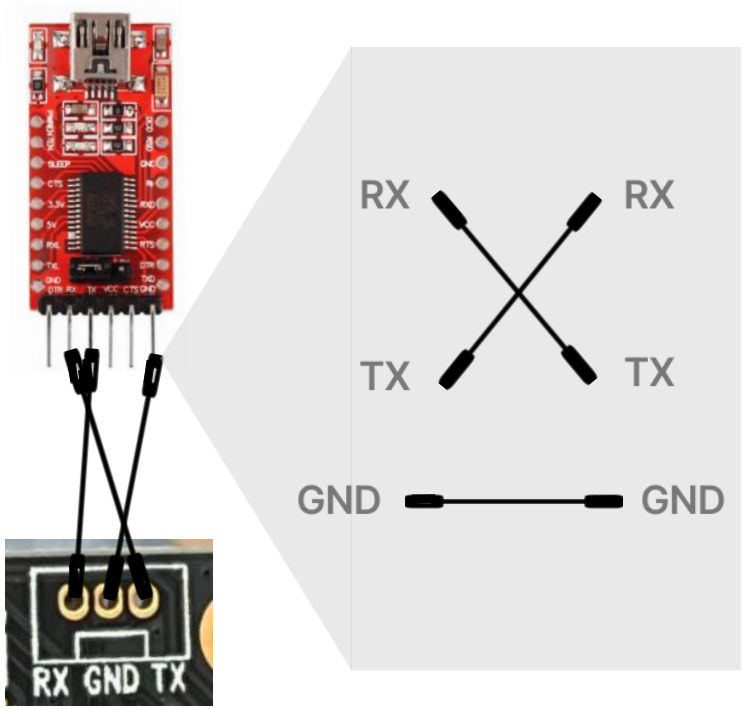


UART PIN 가이드가 있는 PCB

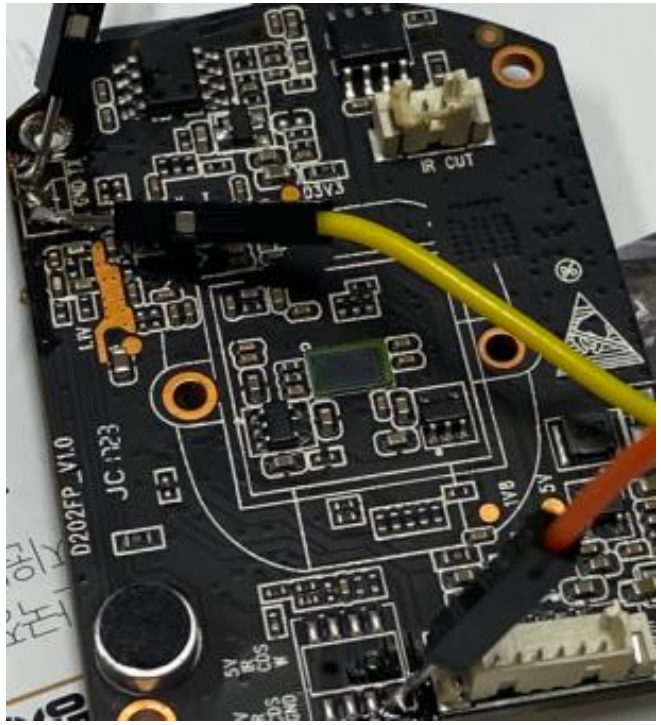


UART PIN 가이드가 없는 PCB

UART Soldering

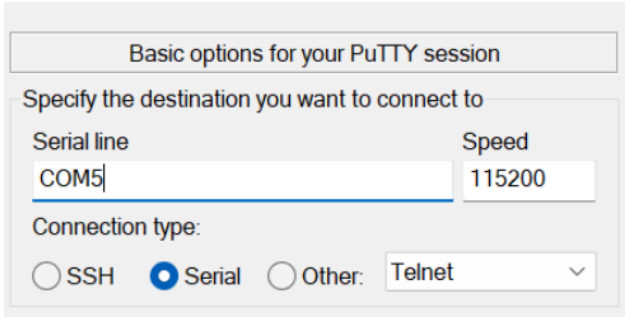


UART Serial 통신

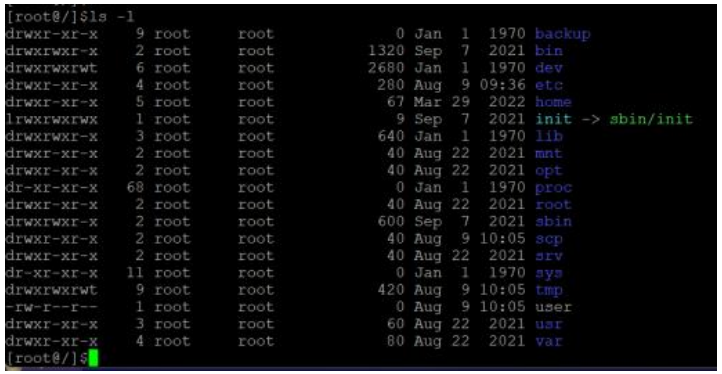


UART PIN 연결

UART Shell 획득 시

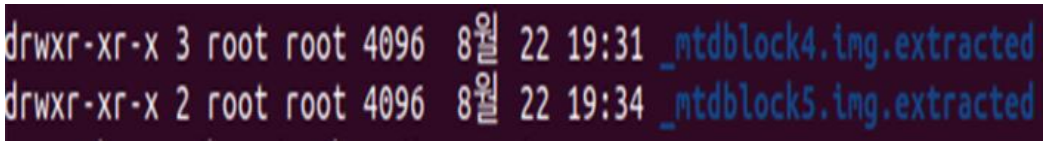


Serial Port와 BaudRate 설정

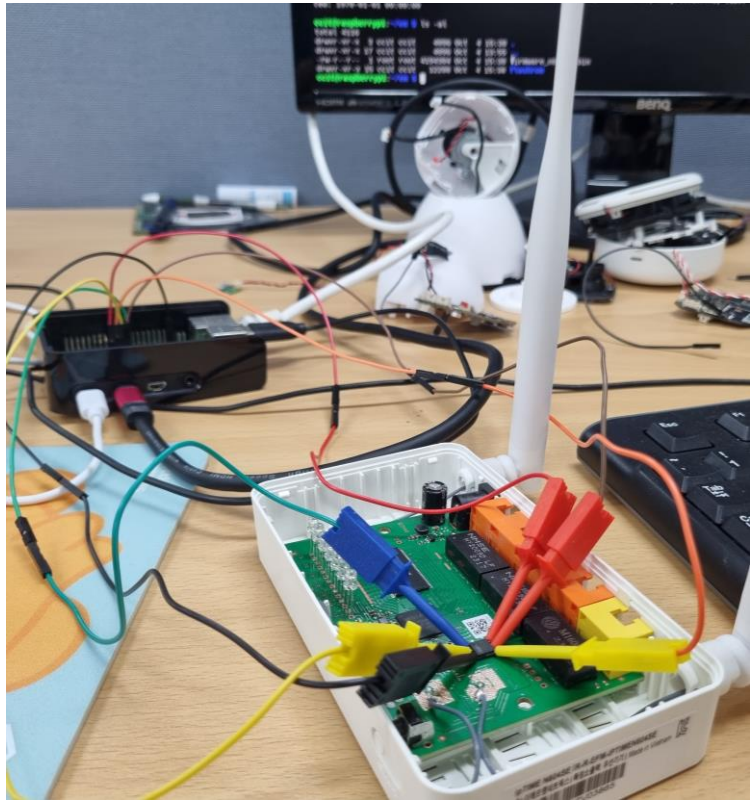


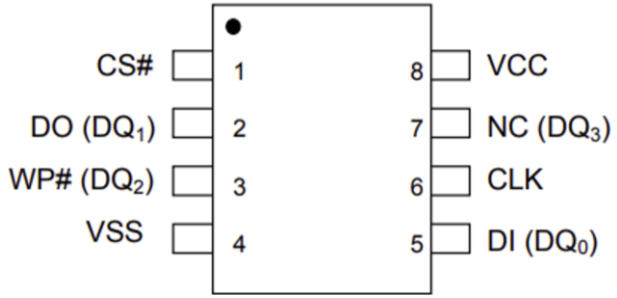
Shell 획득

dd 명령어를 통해 img 파일 덤프 후
Binwalk를 통해 펌웨어 추출

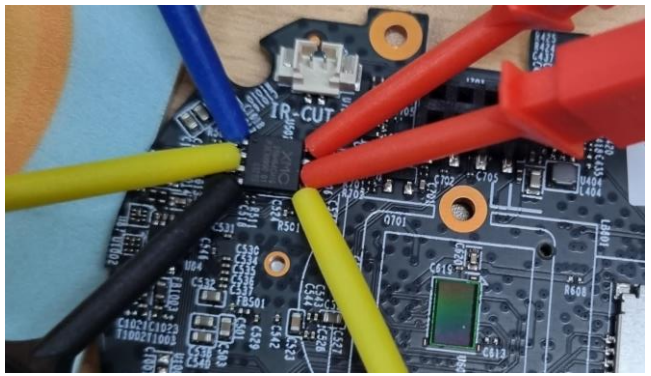


SPI Flashrom Dump



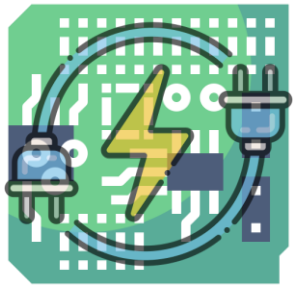


Flash Memory DataSheet



PIN	NAME		NAME	PIN
01	3.3V DC Power		5V DC Power	02
03	GPIO02 (SDA1,I²C)		5V DC Power	04
05	GPIO03 (SDL1,I²C)		Ground	06
07	GPIO04 (GPCLK0)		GPIO14 (TXD0, UART)	08
09	Ground		GPIO15 (RXD0, UART)	10
11	GPIO17		GPIO18(PWM0)	12
13	GPIO27		Ground	14
15	GPIO22		GPIO23	16
17	3.3V DC Power		GPIO24	18
19	GPIO10 (SP10_MOSI)		Ground	20
21	GPIO09 (SP10_MISO)		GPIO25	22
23	GPIO11 (SP10_CLK)		GPIO08 (SPI0_CE0_N)	24
25	Ground		GPIO07 (SPI0_CE1_N)	26
27	GPIO00 (SDA0, I²C)		GPIO07 (SCL0, I²C)	28
29	GPIO05		Ground	30
31	GPIO06		GPIO12 (PWM0)	32
33	GPIO13 (PWM1)		Ground	34
35	GPIO19		GPIO16	36
37	GPIO26		GPIO20	38
39	Ground		GPIO21	40

Raspberry Pi 4 Pinout



Glitch Attack

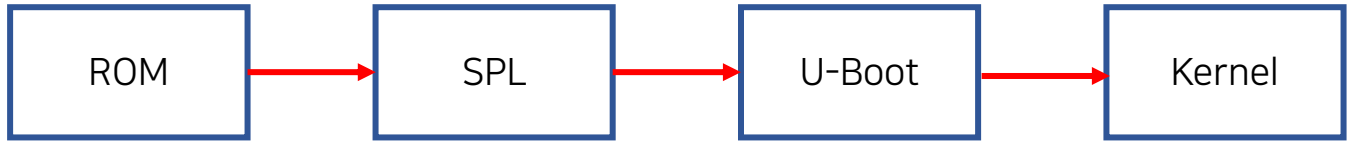
Network

Fuzzing

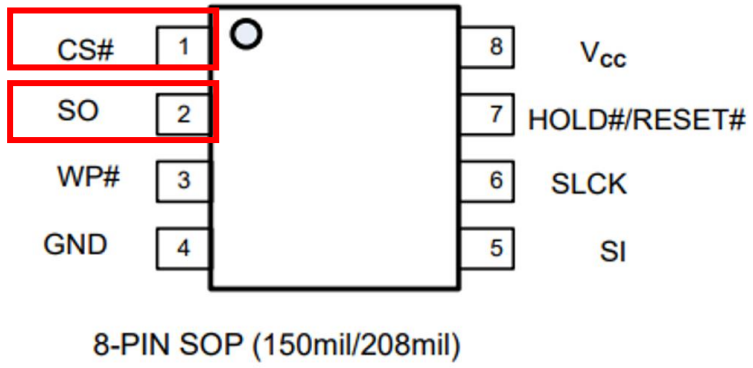
Code Auditing

Glitch Attack

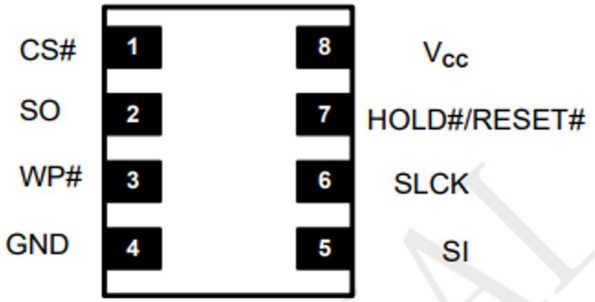
- 임베디드 장비 부팅 순서



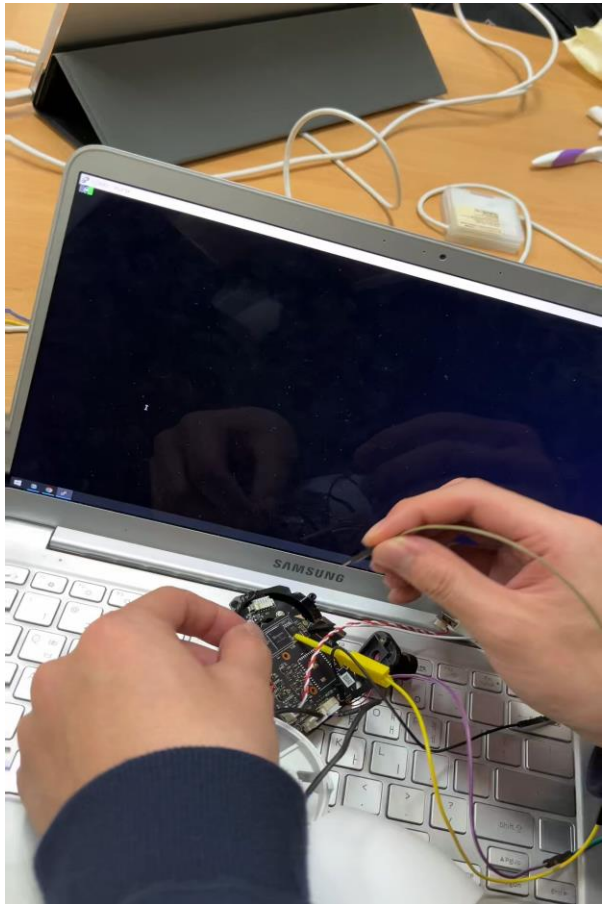
- SPI 데이터시트



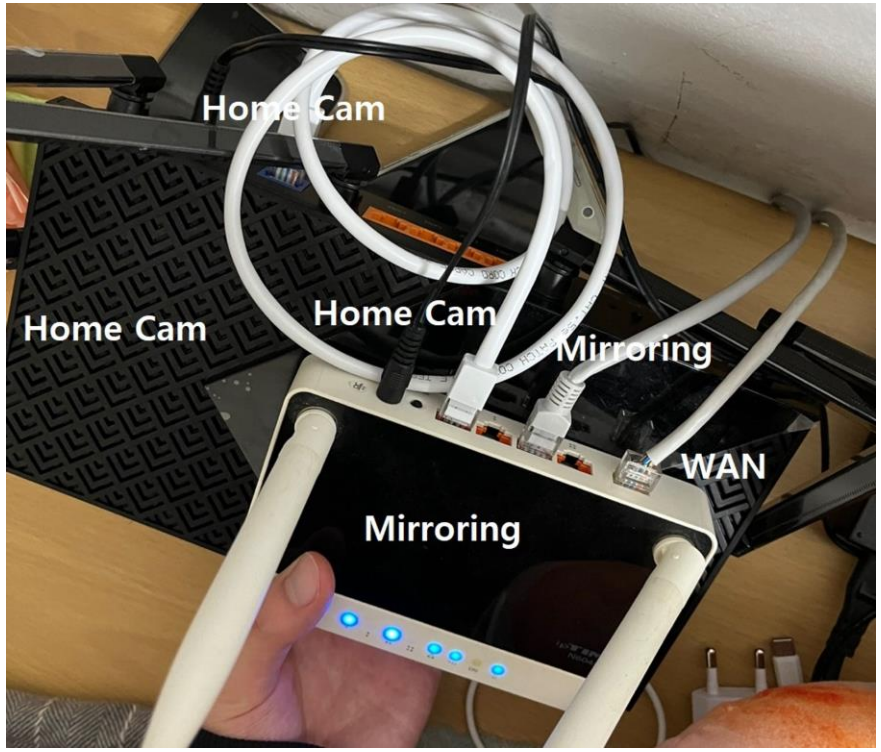
8-PIN SOP (150mil/208mil)



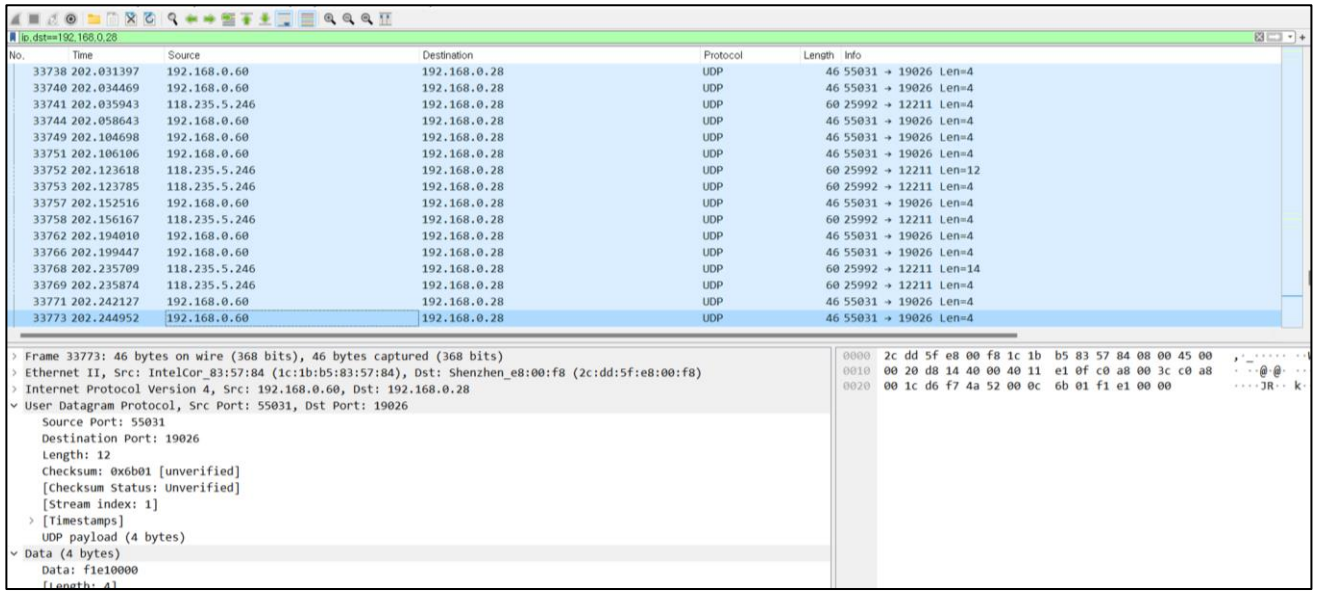
8-Land WSON (6x5mm)



Network



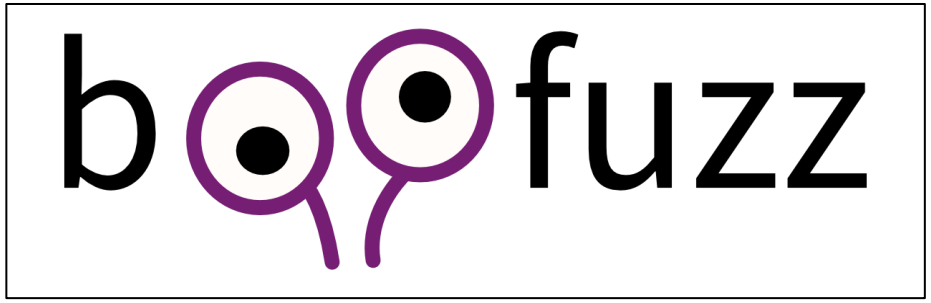
< Port Mirroring >



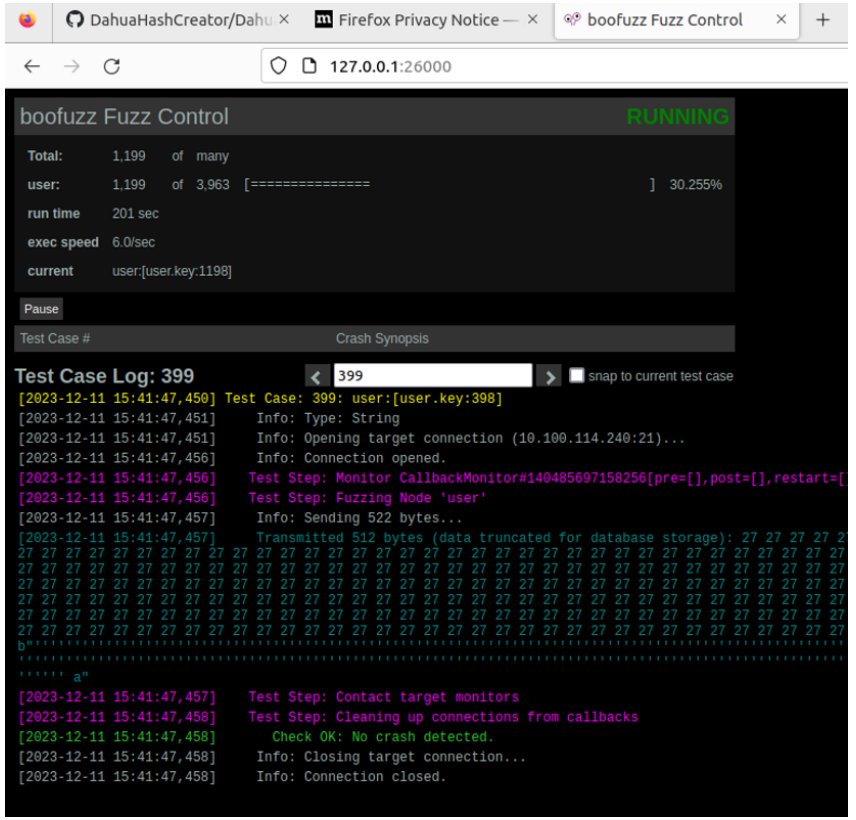
< 패킷 분석 및 Replay 공격 시도 >

Fuzzing

- 소프트웨어의 취약점을 테스트하는 기법
- 소프트웨어에 입력 값을 무작위로 반복적으로 대입
- 입력 시 발생하는 에러나 충돌을 모니터링해서
  보안의 허점을 찾아내는 방식



< boofuzz >



< boofuzz 실행 화면 >

Code Auditing

버그, 보안 위반 또는 프로그래밍 규칙을 위배하는 것을 발견하는 것을 목적으로 **소스 코드를 종합적으로 분석**

IDA -> p2p_tnp 바이너리 분석

```
    source /backup/tools/upgrade.sh

        if [ -f /backup/upgrade_success_flag ];then
                rm /backup/url
                killall rmm
                /tmp/rmm 1 &
                sleep 5
                echo update success will reboot!
        else
                echo update fail will reboot by init.sh update!
        fi

    reboot -f
fi

if [ "${enable_4g}" = "y" ];then
        if [ "${SUFFIX}" = "b221fp" ];then
                /home/app/4g ${GPIO_4G_ENABLE} ${GPIO_4G_VDD} ${GP
                echo "killall 4g" >> /tmp/restart_4g.sh
                echo "/home/app/4g ${GPIO_4G_ENABLE} ${GPIO_4G_VDD
                chmod 777 /tmp/restart_4g.sh
        else
                /home/app/4g &
        fi
fi
export  enable_4g
export NETWORK_IFACE
/home/app/lower_half_init.sh
```

내부 스크립트 파일 분석

H사 IP 카메라 취약점 발견 – Command Injection

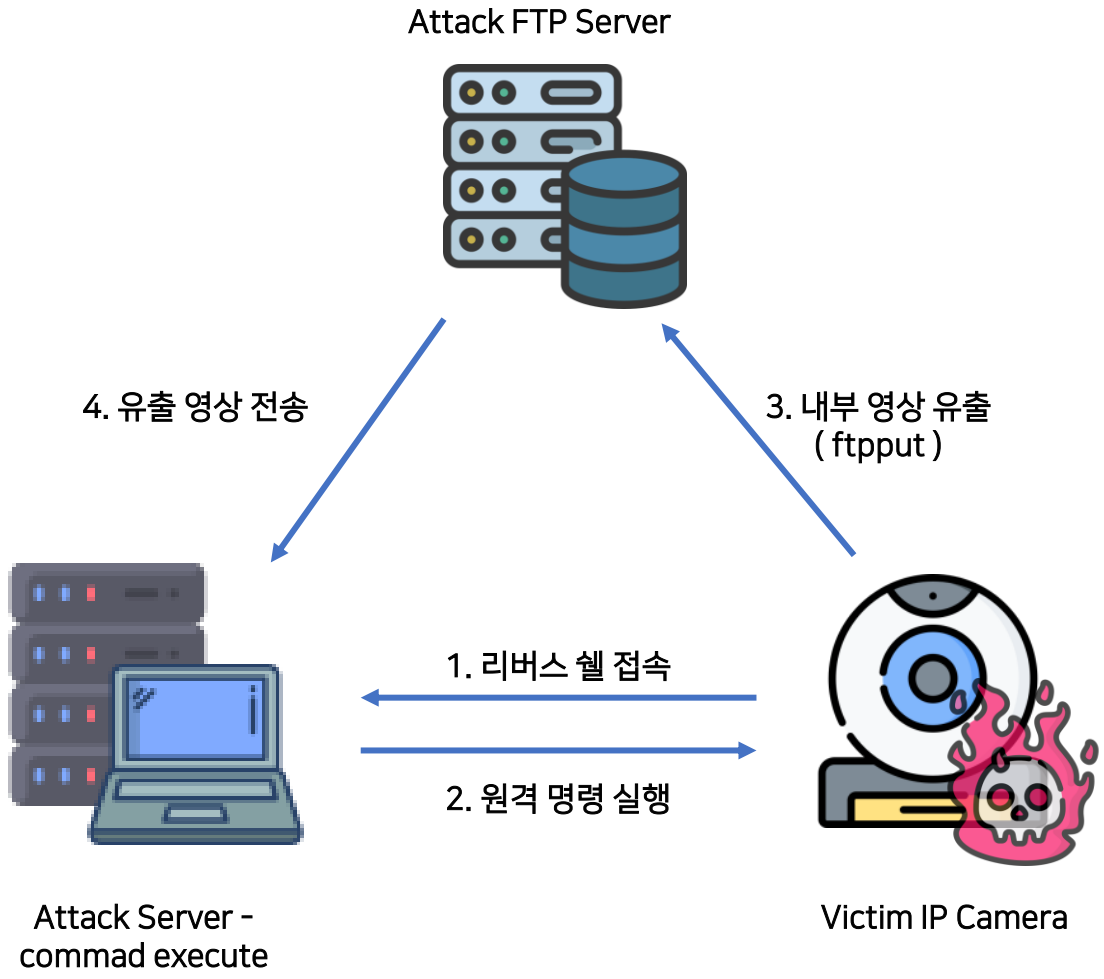
부팅 시 SD Card를 통한
Root 권한 임의 코드 실행 취약점 발견

SD Card로부터 백도어 삽입
(쉘 스크립트 파일 및 취약한 바이너리)

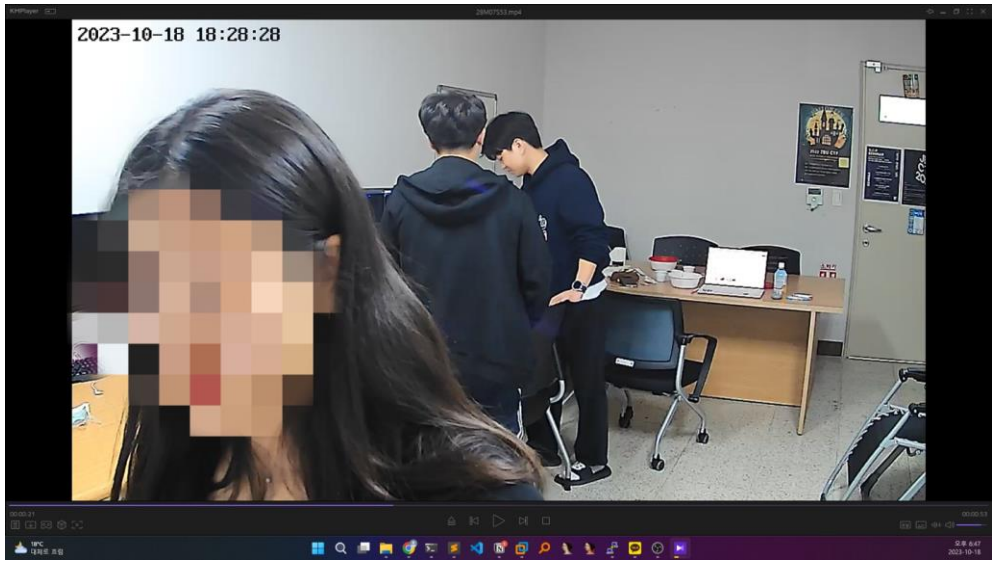
H사 IP 카메라 취약점 발견 – Command Injection

H사 IP 카메라 취약점 발견 – Command Injection

H사 IP 카메라 취약점 검증 – 지속적인 영상 유출



FTP 서버로 전송하여 가져온 홈캠 내부 유출 영상

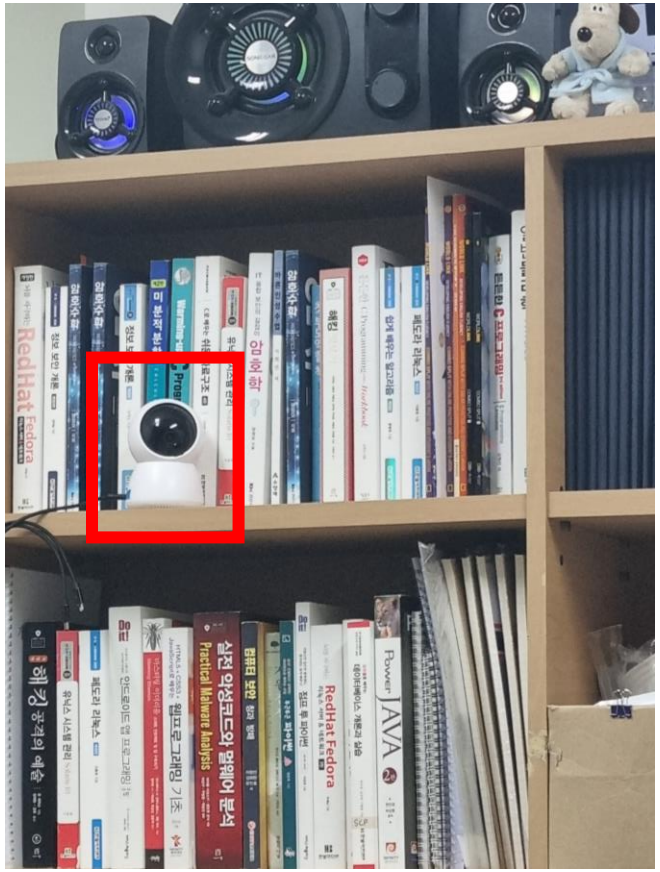


원터치 SD Card 삽입을 통해

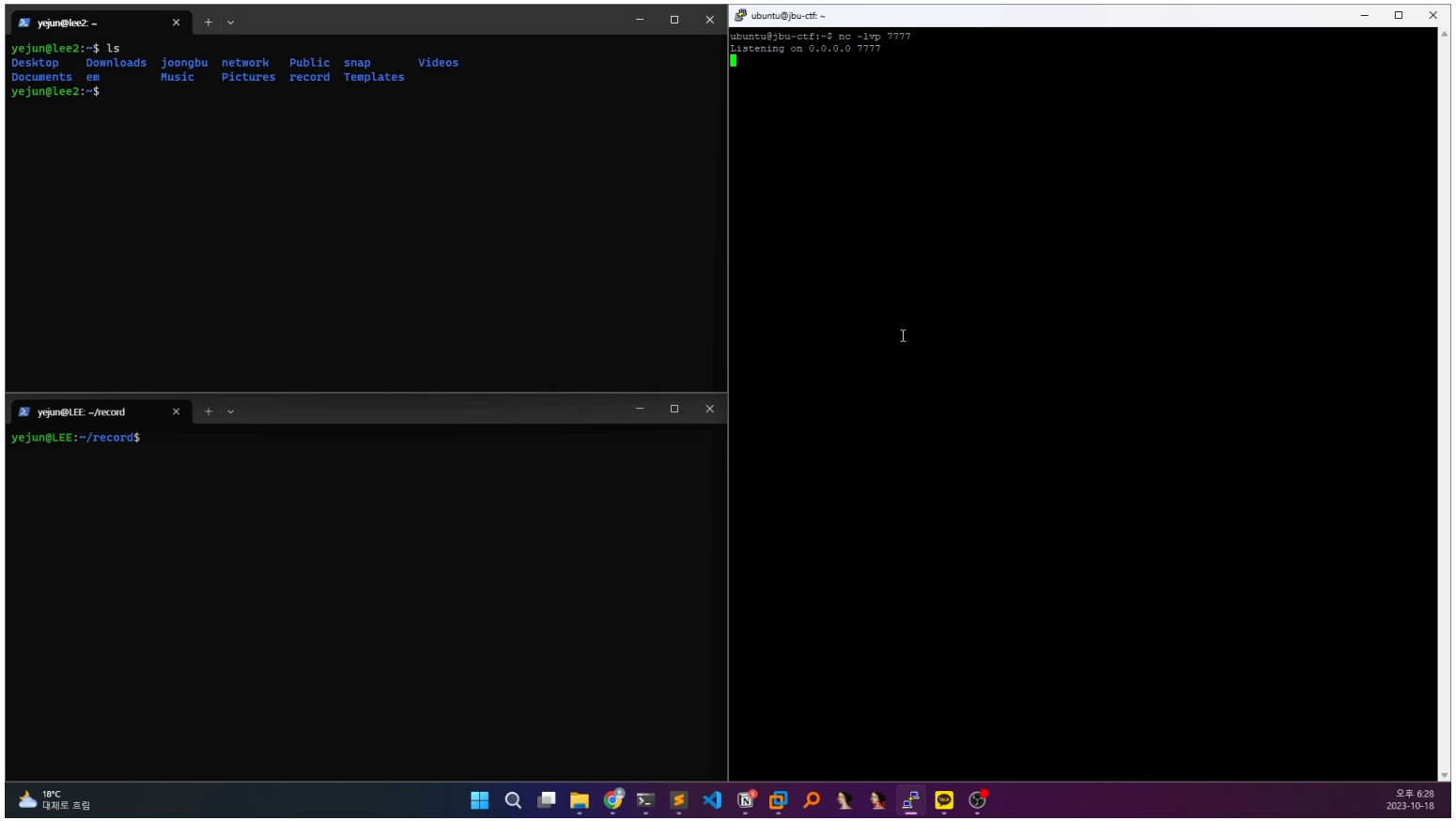
지속적인 영상 유출 피해 발생

But, 사용자는 피해를 인지하지 못함.

H사 IP 카메라 취약점 검증 – 지속적인 영상 유출



< 동아리실 내부 IP 카메라 >



< RCE를 통한 영상 유출 취약점 시연 >

Ⅲ. 프로젝트 결과

H사 IP 카메라 취약점 제보

< KISA 취약점 제보 >

순번	제목	KVE	대상	진행상태	작성자	작성일
1	홈플래닛 IP카메라 커맨드 인젝션을 통한 임의 코드 실행 및 영상 유출 취약점	-	-	평가	exit1100	2023-09-23 01:52:38

[한국인터넷진흥원] '23년 4분기 신고포상제 취약점 평가 결과 및포상금 수령 안내 (이예준) 받은편지함 ×

KVE-2023-5551

한국인터넷진흥원(KISA)
나에게

안녕하세요.
한국인터넷진흥원 보안 취약점 신고포상제 담당자입니다.
신고해주신 '23년 4분기 신고포상제 취약점 평가가 완료되어 평가 결과 및 포상금 수령 안내 드립니다.

네트워크 공격 자동화 도구 제작

임베디드 기기 별로 실행 파일은 코드가 다르지만, 네트워크 스캔 및 공격 요소는 동일함.

Info

- OS : Linux
- 무선 LAN(Wi-Fi) 기반 네트워크 공격 자동화

Menu

1. DoS Attack (Deathentication)
2. Packet Sniffing (include MITM)
3. Packet Replay Attack
4. Port Scanning

네트워크 공격 자동화 도구 개발

-> 임베디드 기기를 분석 시, 네트워크 분석 및 공격을 효율적으로 진행할 수 있음.

네트워크 공격 자동화 도구 제작

```
yejun@lee2:~/network/deauth-attack_bak/src$ ./death-attack
syntax: deauth-attack <interface>
sample: deauth-attack wlan0

yejun@lee2:~/network/deauth-attack_bak/src$ sudo ./death-attack wlx88366cfba604
[sudo] password for yejun:
1. AP Scanning
2. Station Scanning
3. Deathentication Attack
0. Exit Program
>>
```

- Wifi Scan(1~2번)은 aircrack-ng 도구를 이용하여 구현
- death attack(3번)은 pcap을 이용하여 직접 구현 (C언어)

DoS Attack (Deathentication)

```
[*] input option (0~5) >> 2
lo        no wireless extensions.

ens33     no wireless extensions.

wlx88366cfba604  IEEE 802.11  Mode:Monitor  Frequency:2.432 GHz  Tx-Power=20 dBm

          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

[*] interface >> wlx88366cfba604
[*]       Station IP >> 192.168.1.20
[*]       AP IP >> 192.168.1.1
```

ARP 스푸핑 후, 필터 조건을 통한 패킷 스니핑 도구

Packet Sniffing (include MITM)

Packet Replay Attack

```
[*] input option (0~2) >> 2

[*] Pcap File List
[0] Exit
[1] 20231122202423.pcap
[2] 20231122174318.pcap
[3] 20231122173928.pcap
[4] 20231122174024.pcap
[5] 20231122174558.pcap
[6] 20231123095853.pcap
[*] input pcap number >> 6
[6] 20231123095853.pcap Packet Replay !
.....
.....
.....
.....
.....
.....
Sent 663 packets.
```

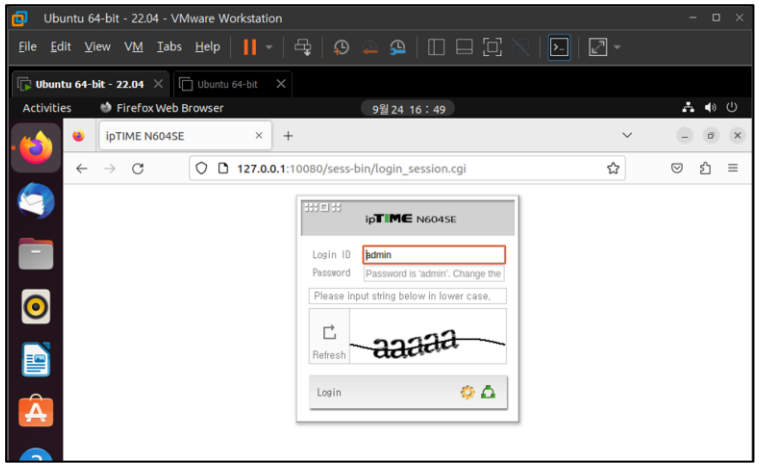
패킷을 캡처하거나 캡처된 패킷을 Replay 해주는 도구

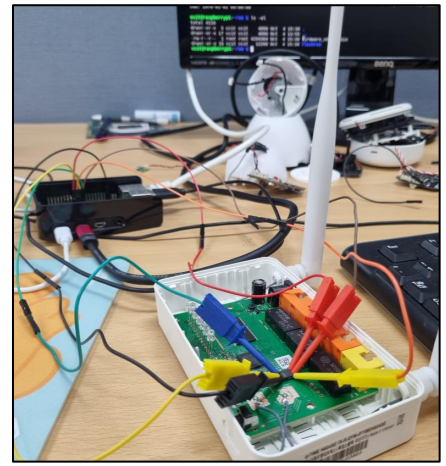
Port Scanning

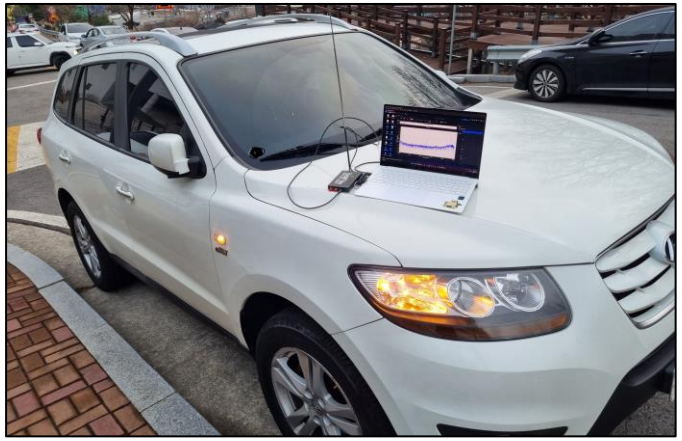
```
[*] input option (0~5) >> 4
[*] ip >> 192.168.1.1

[*] Port Scanning
[1] TCP
[2] UDP
[0] exit

[*] input option (0~2) >>
```

Port Scan 도구 (nmap 활용)

임베디드 기기 분석 능력 향상







- 하드웨어 작업 능력 향상 (**납땜, 회로** 구성)
- 추후 **다양한 임베디드 기기 분석 및 연구** 가능
- 하드웨어 장비 **에뮬레이팅** 기술 습득
- 파이썬 **자동화 도구 개발** 능력 향상

향후 계획

- 4학년 졸업 프로젝트에서 **다양한 임베디드 기기에 대한 분석과 연구**를 진행해볼 예정

- 다양한 연구 진행 시, 임베디드 관련 **논문 작성** 예정 (학회 투고 및 발표)

- 네트워크 공격 자동화 도구 개발 **사용자 친화적인 GUI 개발 계획** 수립 중.. (확정은 아님)

- **IoT 관련 개발 프로젝트**를 진행하는 팀이나 기업이 있다면, **보안적인 관점에서 분석 및 협업** 가능

질문 있으신가요?

감사합니다