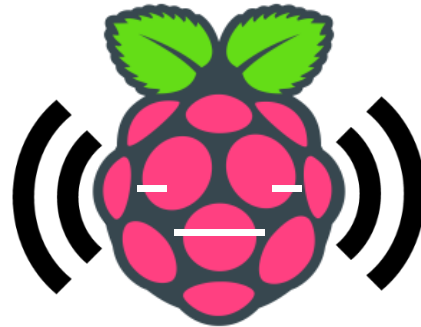


Evil Twin Attack

with Captive Portal



황선홍(fkillrra)
f.killrra@gmail.com

Agenda

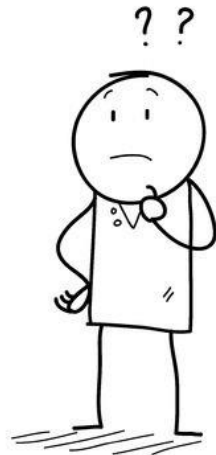
- Abstract
 - 동기
 - 문제점 및 해결 방안
 - 결론
- Contents
 - 개요
 - 관련 기술 소개
 - 결과 및 향후 계획

Abstract - 동기

- WiFi 연결 방식

공공장소에서 WiFi를 이용할 때
연결이 끊기지 않고 이용이 가능하다.

ex) 지하철, 도서관, 학교 등



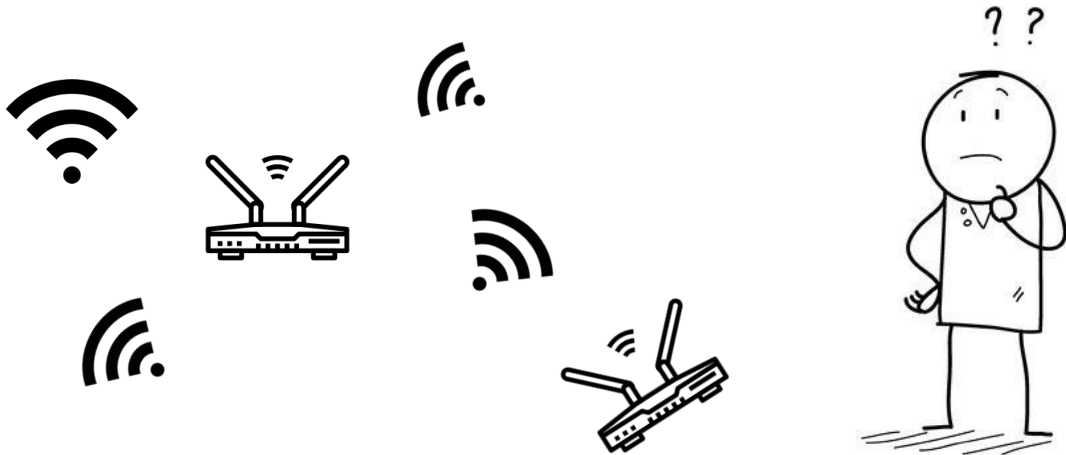
Abstract - 동기

- WiFi 연결 방식

공공장소에서 WiFi를 이용할 때
연결이 끊기지 않고 이용이 가능하다.

ex) 지하철, 도서관, 학교 등

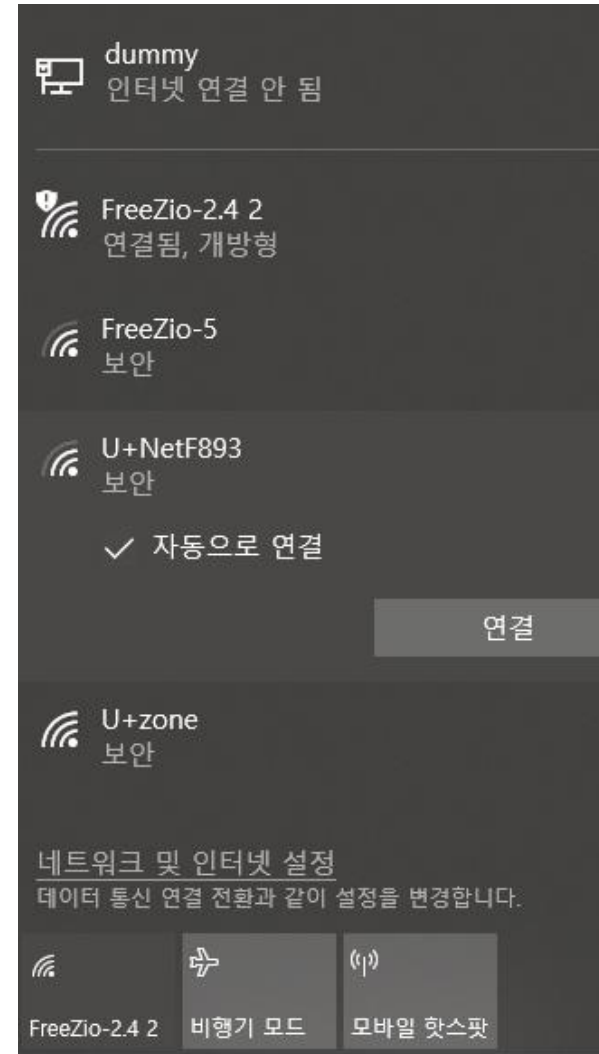
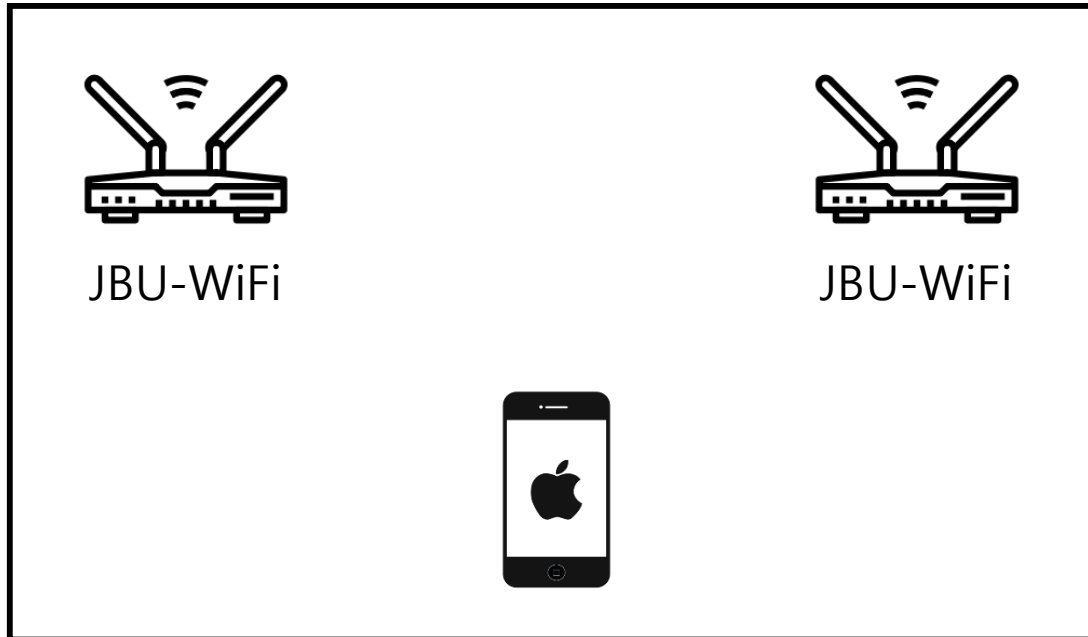
이유 : 같은 이름의 WiFi가 여러곳에 존재하기 때문!



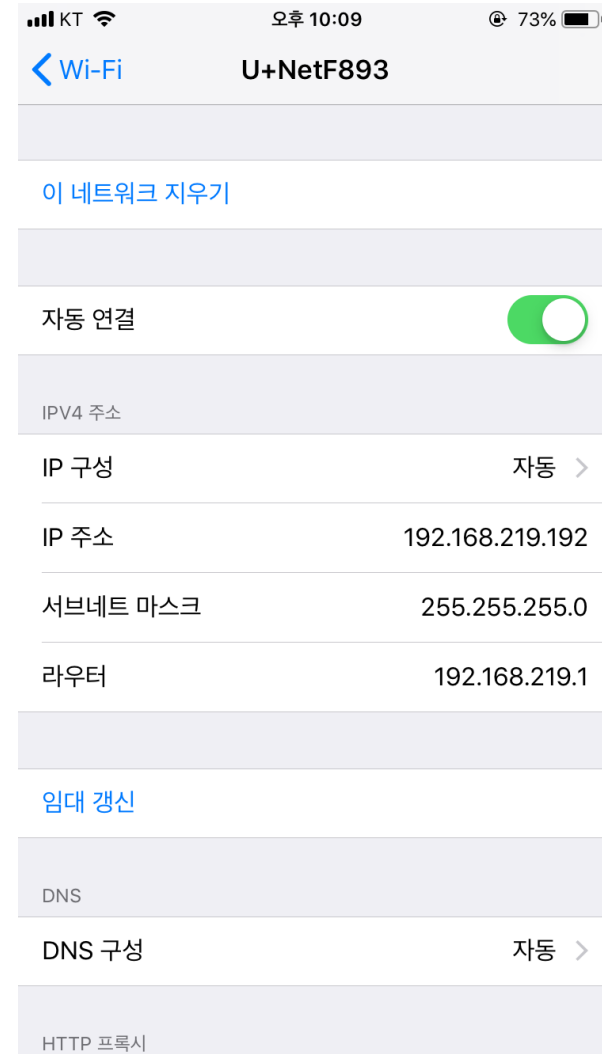
Abstract - 동기

- WiFi 연결 방식

station은 자동연결이라는 기능을 통해
연결이 끊기지 않고 wifi를 이용할 수 있다.



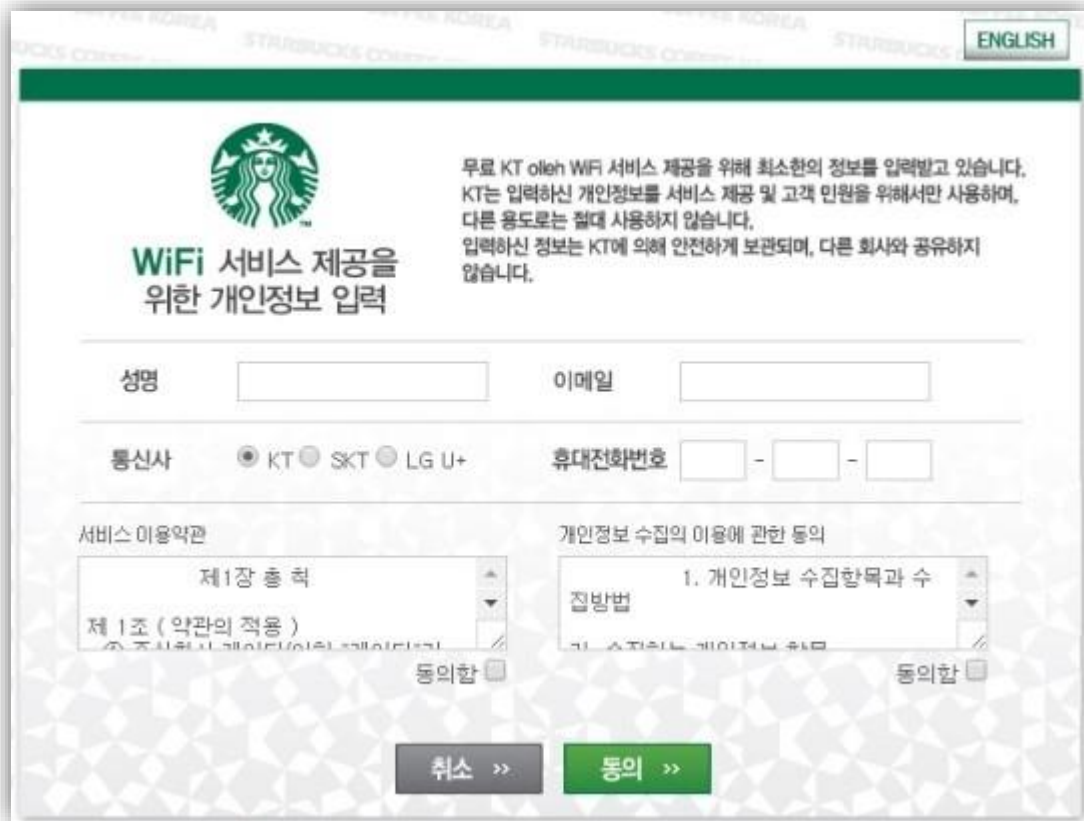
windows 10



iphone

Abstract - 동기

- Captive Portal



Starbucks WiFi 서비스 제공을 위한 개인정보 입력

무료 KT olleh WiFi 서비스 제공을 위해 최소한의 정보를 입력받고 있습니다. KT는 입력하신 개인정보를 서비스 제공 및 고객 민원을 위해서만 사용하며, 다른 용도로는 절대 사용하지 않습니다. 입력하신 정보는 KT에 의해 안전하게 보관되며, 다른 회사와 공유하지 않습니다.

성명 이메일

통신사 ☒ KT ☐ SKT ☐ LG U+ 휴대전화번호 - -

서비스 이용약관 제1장 총칙
제 1 조 (약관의 적용)
본 조항은 서비스 제공을 위한 개인정보 수집, 처리, 보유, 이용에 관한 사항을 규정합니다.

개인정보 수집의 이용에 관한 동의
1. 개인정보 수집항목과 수집방법
본 서비스는 개인정보를 수집합니다.

☐ 동의함 ☐ 동의함

[Starbucks]



Wi-Fi

ollehWiFi

네트워크 선택...

CONFIG_LAB

hunusbio 3F

olleh_real

olleh_starbucks

ollehWiFi

Seoul WiFi

기타...

olleh WiFi zone

olleh WiFi에 오신 고객님 환영합니다.
이벤트 및 알림정보 등 다양한 혜택을 제공하는 것에 동의하십니까?

서비스 이용약관

기사회생 맨유가 꿈꿔야 할 '리슨 기적'

매우 큰 '기적'의 순간, 카가와는 안았다

[Olleh WiFi zone]

Abstract - 문제점 및 해결 방안

[문제점]

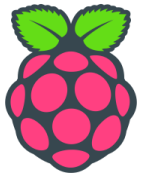
1. AP mode의 지원 여부
 - 제조사의 칩셋에 따라 사용할 수 있는 모드가 제한적이다.
2. Uplink 유/무선
 - 인터넷에 직접적으로 연결이 되는 Uplink가 유선일 경우 설치가 어렵다.

Abstract - 문제점 및 해결 방안

[문제점]

1. AP mode의 지원 여부
 - 제조사의 칩셋에 따라 사용할 수 있는 모드가 제한적이다.
2. Uplink 유/무선
 - 인터넷에 직접적으로 연결이 되는 Uplink가 유선일 경우 설치가 어렵다.

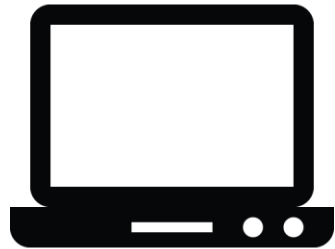
[해결 방안]



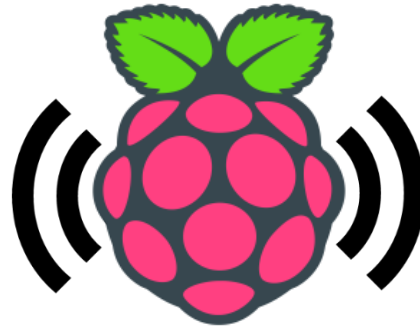
- 라즈베리파이3의 내장된 랜카드는 AP mode를 지원한다.
- 무선 랜카드를 이용하여 Uplink를 무선으로 설정한다.

Abstract - 결론

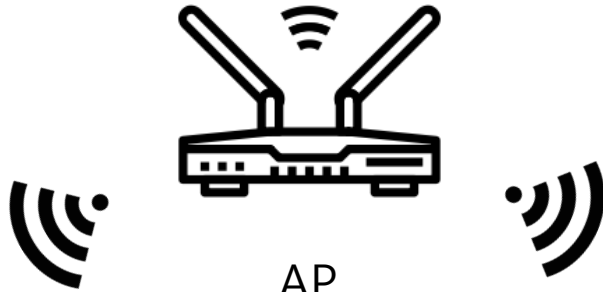
[구상도]



Laptop



AP



Smart Phone

Contents - 개요

1. Raspberry Pi3를 이용하여 공유기를 만든다.



2. Deauthentication Attack으로 이미 연결되어있는 AP의 연결을 해제한다.

3. 접속된 Station을 Captive portal로 redirect 해준다.

Contents - 관련 기술 소개

- Evil Twin Attack
- Wi-Fi Deauthentication Attack
- Captive Portal

Evil Twin Attack

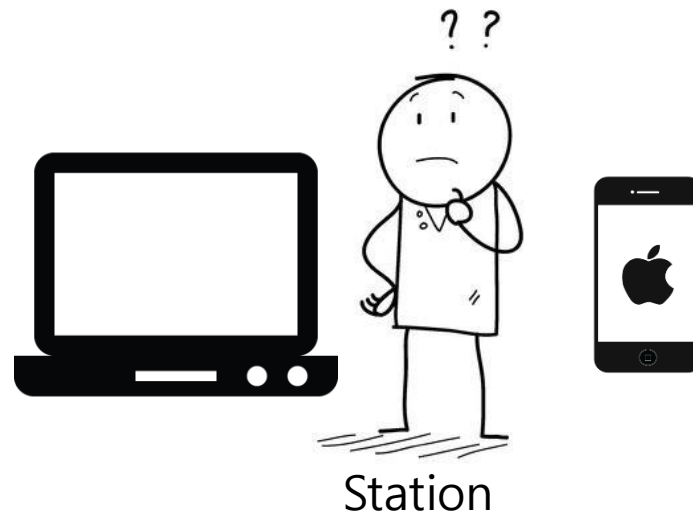
동일한 SSID를 갖은 AP를 이용해 무선 LAN
환경에서 통신을 도청하도록 설정하여 공격
하는 방식



Real AP(SSID : JBU-WiFi)



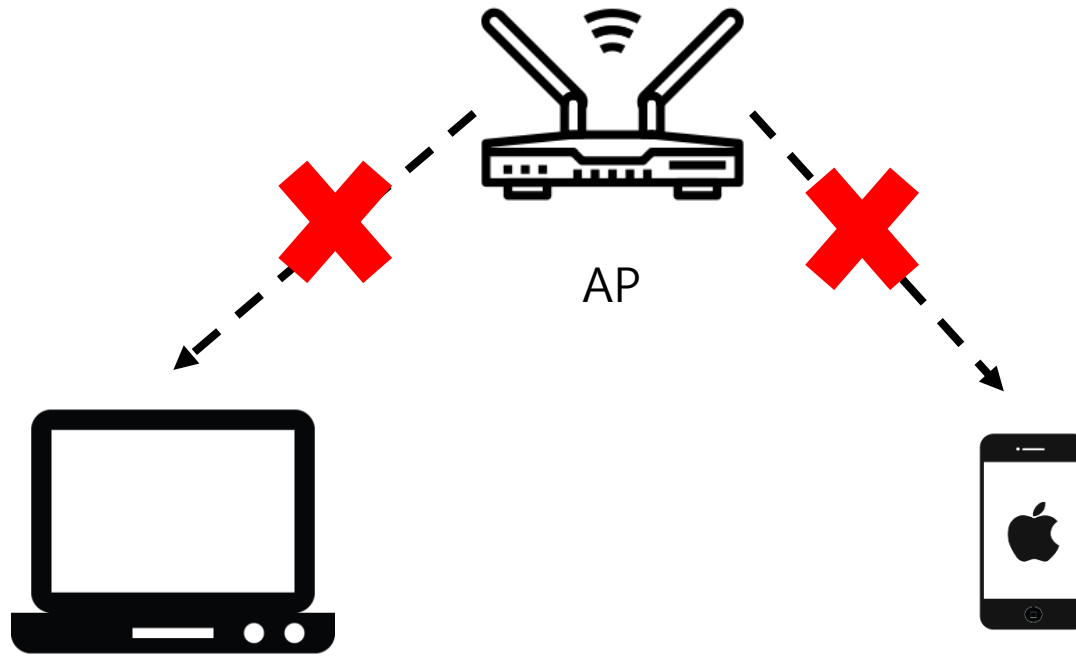
Rogue AP(SSID : JBU-WiFi)



사용자는 어떤 AP가 진짜인지
구별할 수 없고,
악의적인 AP에 연결함으로써
모든 통신을 도청당하게 된다.

WiFi Deauthentication Attack

- 사용자와 AP간의 연결을 끊어주는 패킷



Captive Portal

- 목적에 따라 다양한 형태로 존재
- 개방형 무선 네트워크에서 주로 사용됨

결과 및 향후 계획

- 데모 영상

결과 및 향후 계획

- 자동화 프로그램 개발
- 소형화 및 휴대성 증가
- 논문 작성, 정보보호 학회 제출

Q&A

Thank you

Thanks to 이경문 교수님

Thanks to 표상영