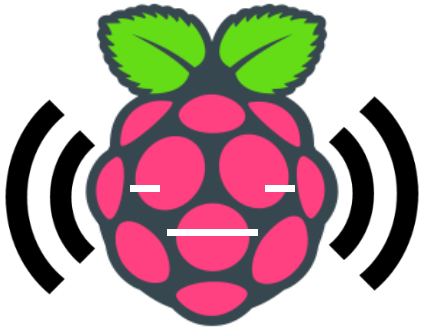
CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

2018년 2학기 CCIT 프로젝트 발표회

Evil Twin Attack

with Captive Portal



황선홍(fkillrra)
f.killrra@gmail.com

2019-01-15

Agenda

- Abstract

- Introduction
  - What is Evil Twin Attack?
  - What is Captive Portal?
  - What is Deauthentication Attack?

- Method & Experiment
  - How to build Evil Twin Access Point & Captive Portal

- Demo & Plan

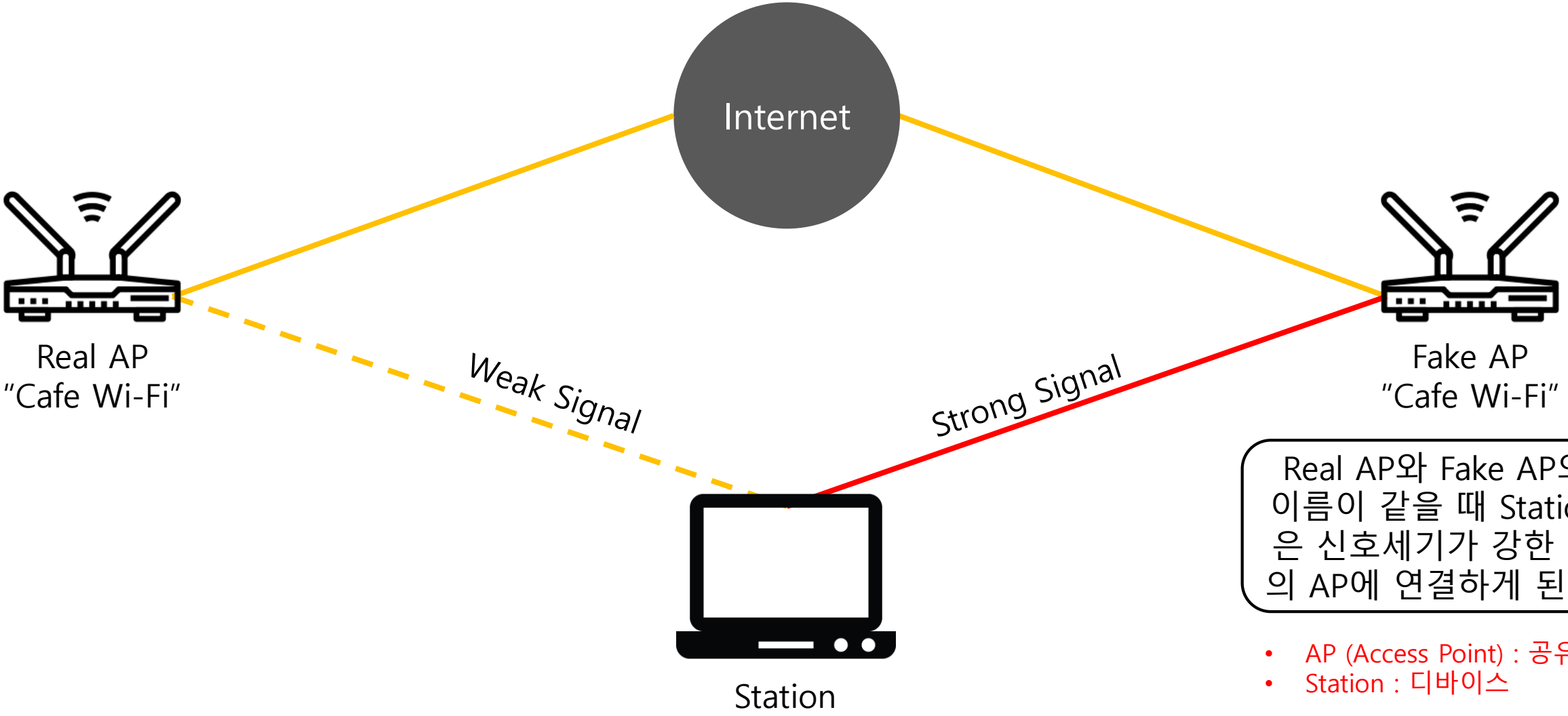
Abstract

BlackHat USA에서 발표된 Evil Twin Attack을 이용하여 Public WiFi의 취약성을 진단한다.

무선 네트워크의 보안 위협에도 불구하고 공공장소 혹은 가정에서 쉽게 개방형 WiFi를 찾아볼 수 있다.

이 프로젝트는 Evil Twin AP를 만들고, 이 AP에 Captive Portal 서비스를 이용하여 사용자의 개인정보를 탈취하는 시나리오로 진행된다.

What is Evil Twin Attack?



Real AP와 Fake AP의 이름이 같을 때 Station은 신호세기가 강한 쪽의 AP에 연결하게 된다.

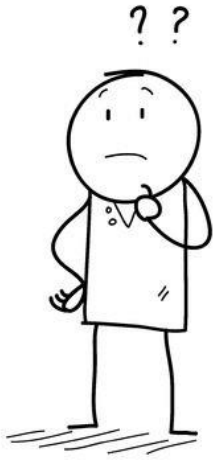
- AP (Access Point) : 공유기
- Station : 디바이스

What is Evil Twin Attack?

- WiFi 연결 방식

공공장소에서 WiFi를 이용할 때
연결이 끊기지 않고 이용이 가능하다.

ex) 지하철, 도서관, 학교 등



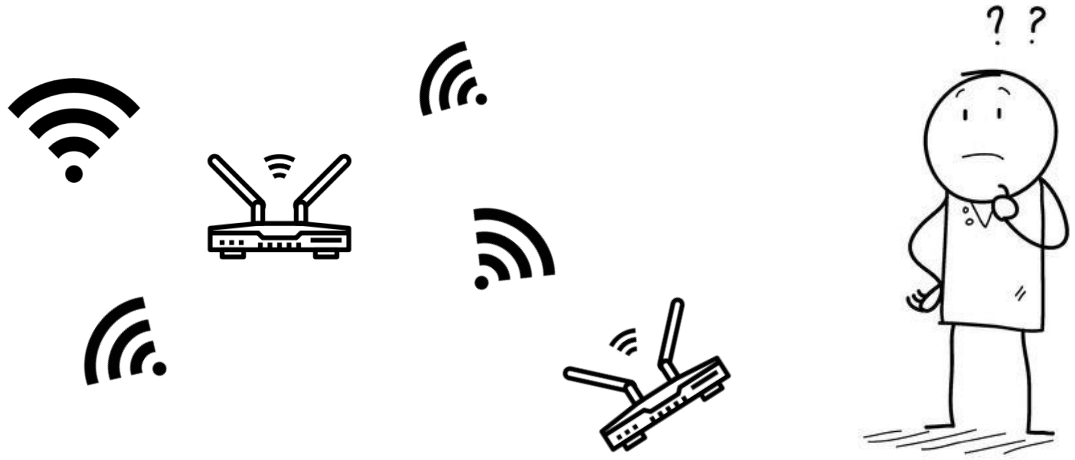
What is Evil Twin Attack?

- WiFi 연결 방식

공공장소에서 WiFi를 이용할 때
연결이 끊기지 않고 이용이 가능하다.

ex) 지하철, 도서관, 학교 등

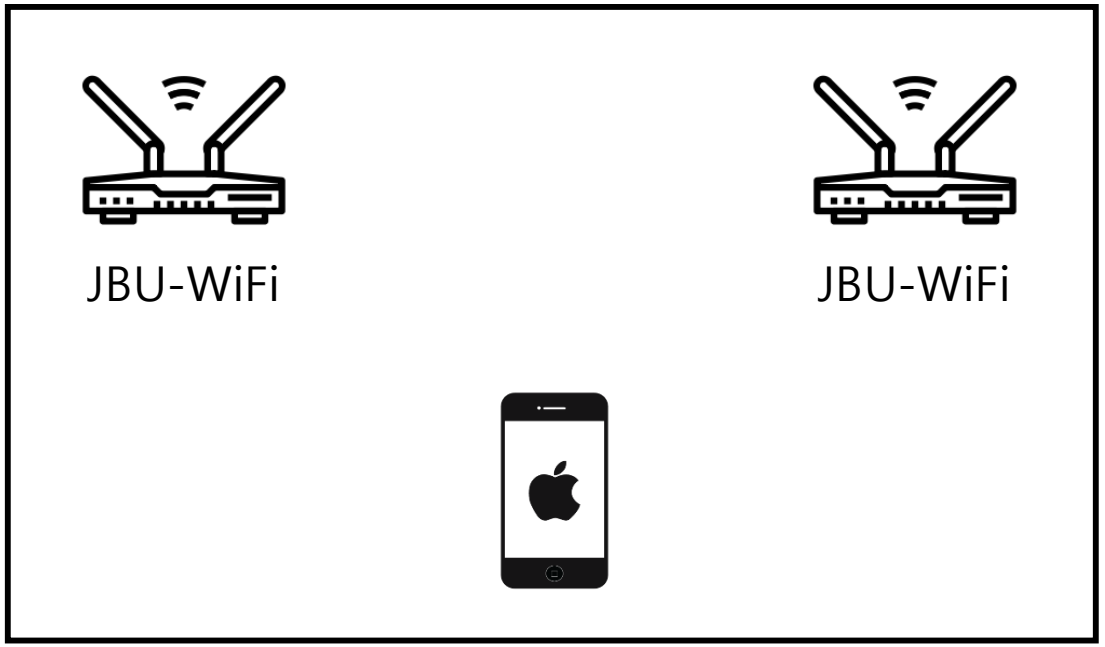
이유 : 같은 이름의 WiFi가 여러곳에 존재하기 때문!



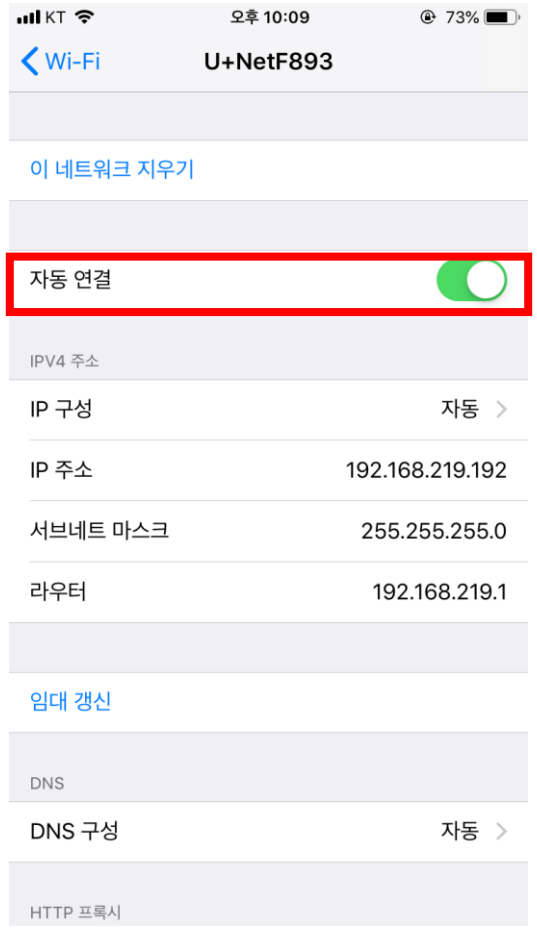
What is Evil Twin Attack?

- WiFi 연결 방식

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

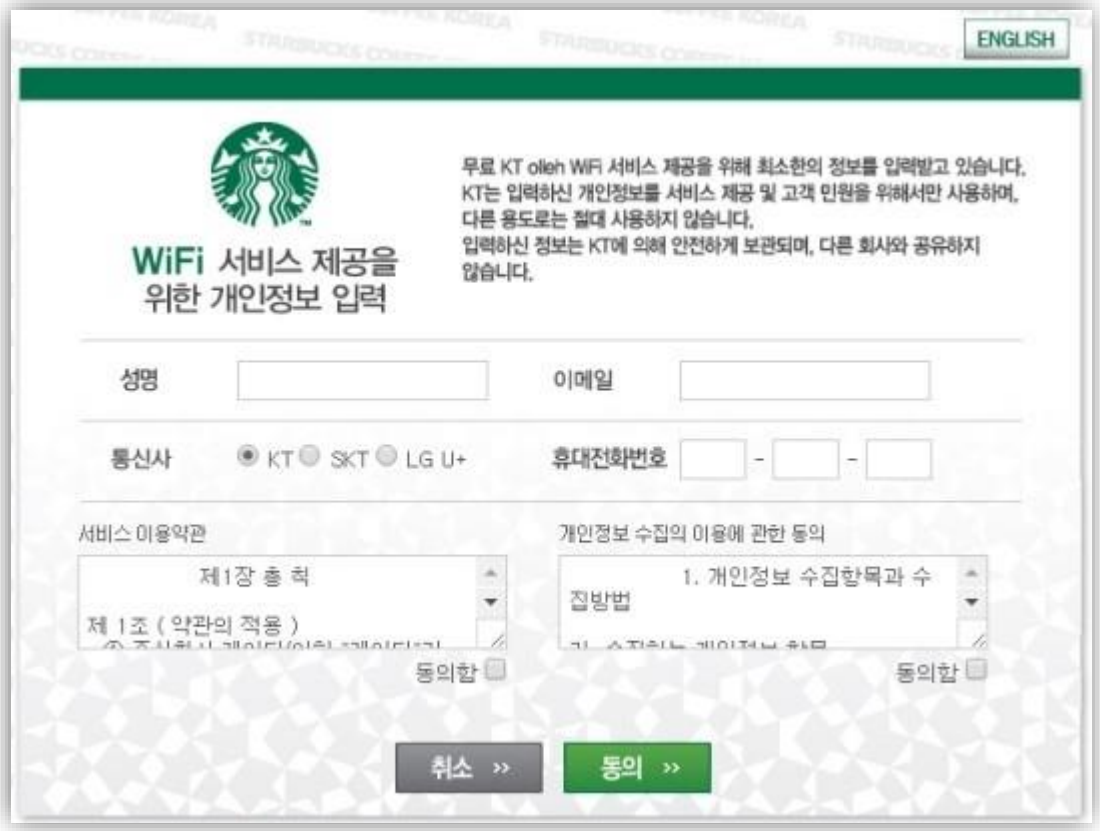


windows 10



iphone

What is Captive Portal?

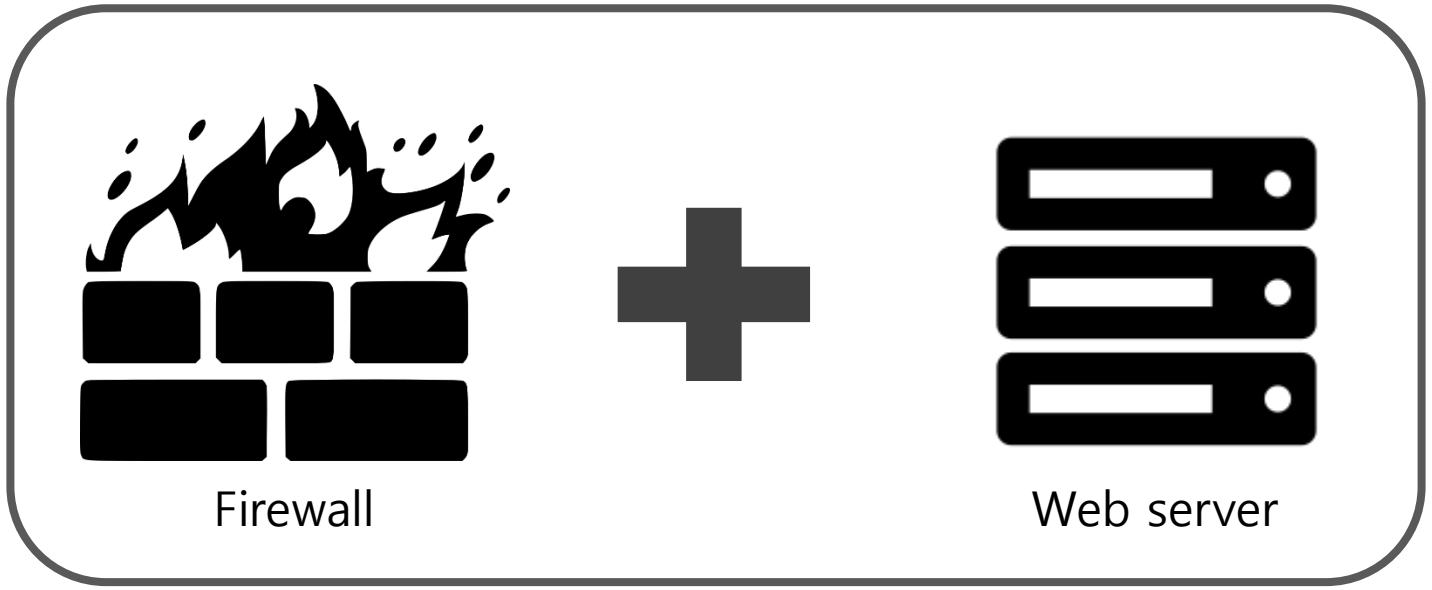


[Starbucks]

[Olleh WiFi zone]

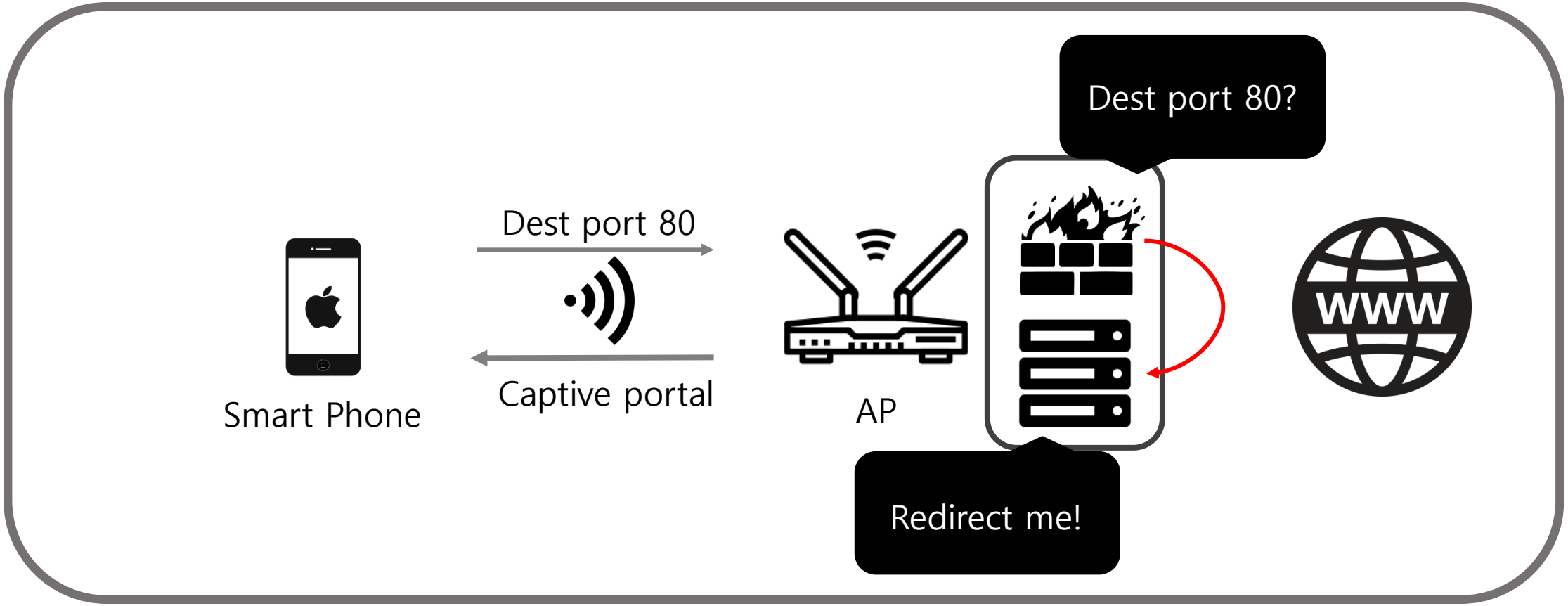
What is Captive Portal?

Captive Portal = 방화벽 + 웹서버



What is Captive Portal?

- 개방형 무선 네트워크에서 주로 사용된다.
- 마케팅 및 상업 커뮤니케이션 목적으로 사용되는 경우가 많다. (광고 목적)



How to build Evil Twin Access Point?

[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.

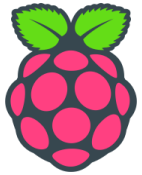
How to build Evil Twin Access Point?

[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.

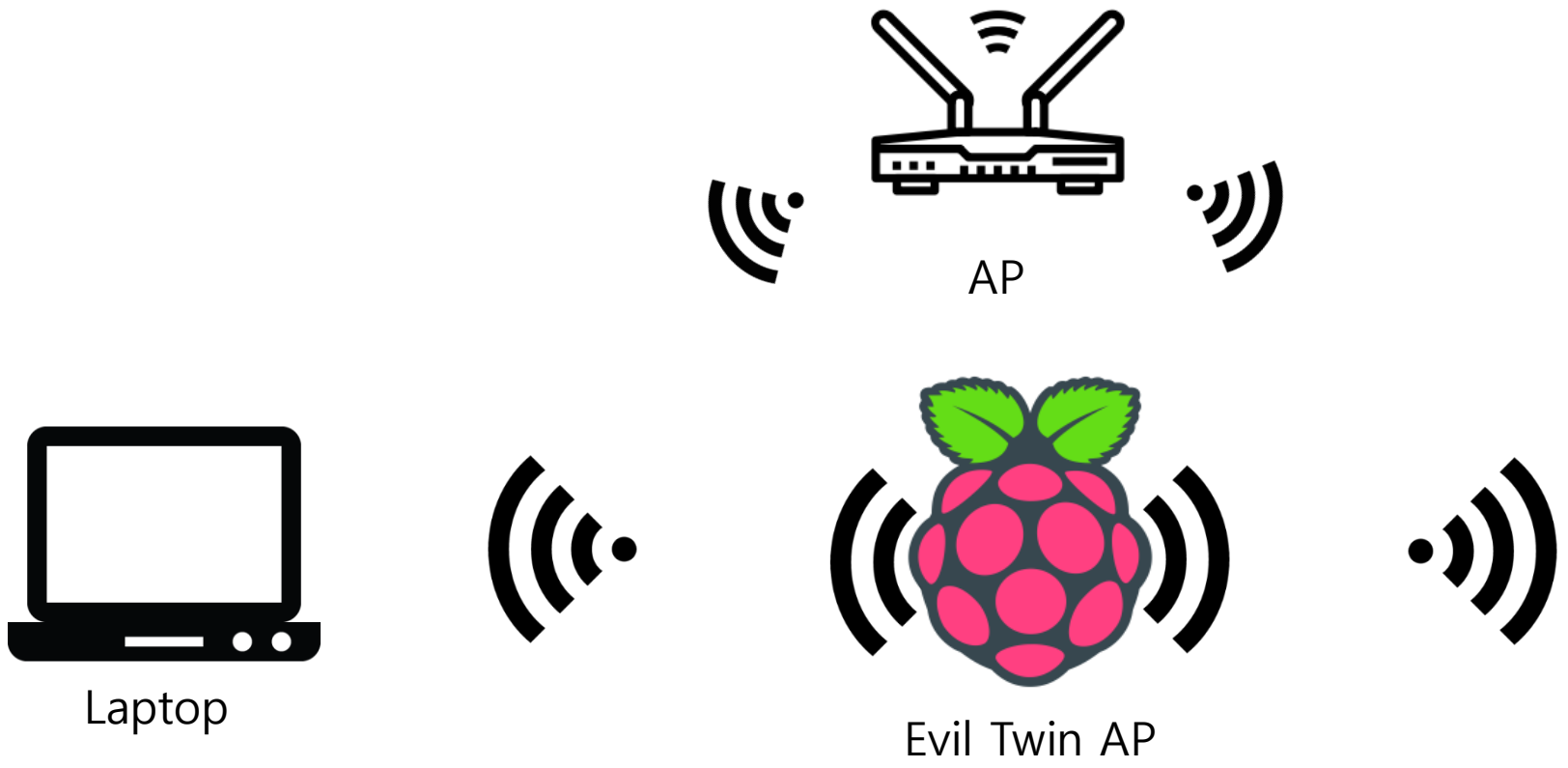
[해결 방안]



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

How to build Evil Twin Access Point?

[구상도]



How to build Evil Twin Access Point?

1. Raspberry Pi3를 이용하여 공유기를 만든다.

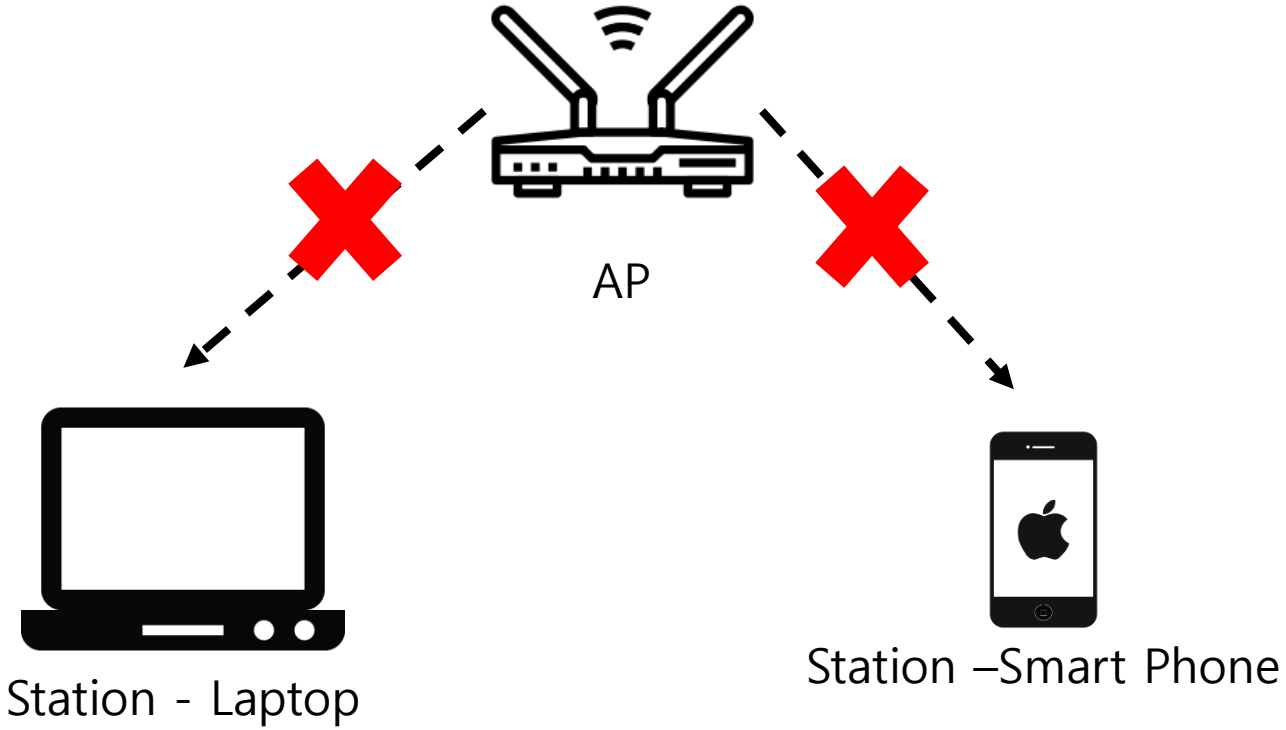
2. Deauthentication Attack으로 이미 연결되어있는 AP의 연결을 해제한다.

3. 자동으로 접속된 Station을 Captive portal로 redirect 해준다.

WiFi Deauthentication Attack

기존의 연결된 AP의 연결을 해제하기 위함

- 무선 네트워크에서 Station과 AP간의 연결을 끊어주는 공격



Demo

Plan

- 자동화 프로그램 개발
- 소형화 및 휴대성 증가

- 논문 작성, 정보보호 학회 제출

Q&A

Thank you

Thanks to 이경문 교수님
Thanks to 표상영