Hacking Wireless Networks Via Evil Twin Attack

—

Created By Amir Mansurian

Contents

- **Wi-Fi Hacking**
- **What Is Evil Twin Attack ?**
- **How To perform Attack?**
- **Defending Against Evil Twin Attack**

Wi-Fi Hacking

Wi-Fi Hacking

- Wi-Fi Networks can be setup by smart IT people, but users are usually Ordinary people without enough Knowledge

- Stealing Wi-Fi passwords is possible with kicking user of from trusted network while creating identical fake one

- More Technical people recognize this, but it is surprisingly Effective

Evil Twin Attack

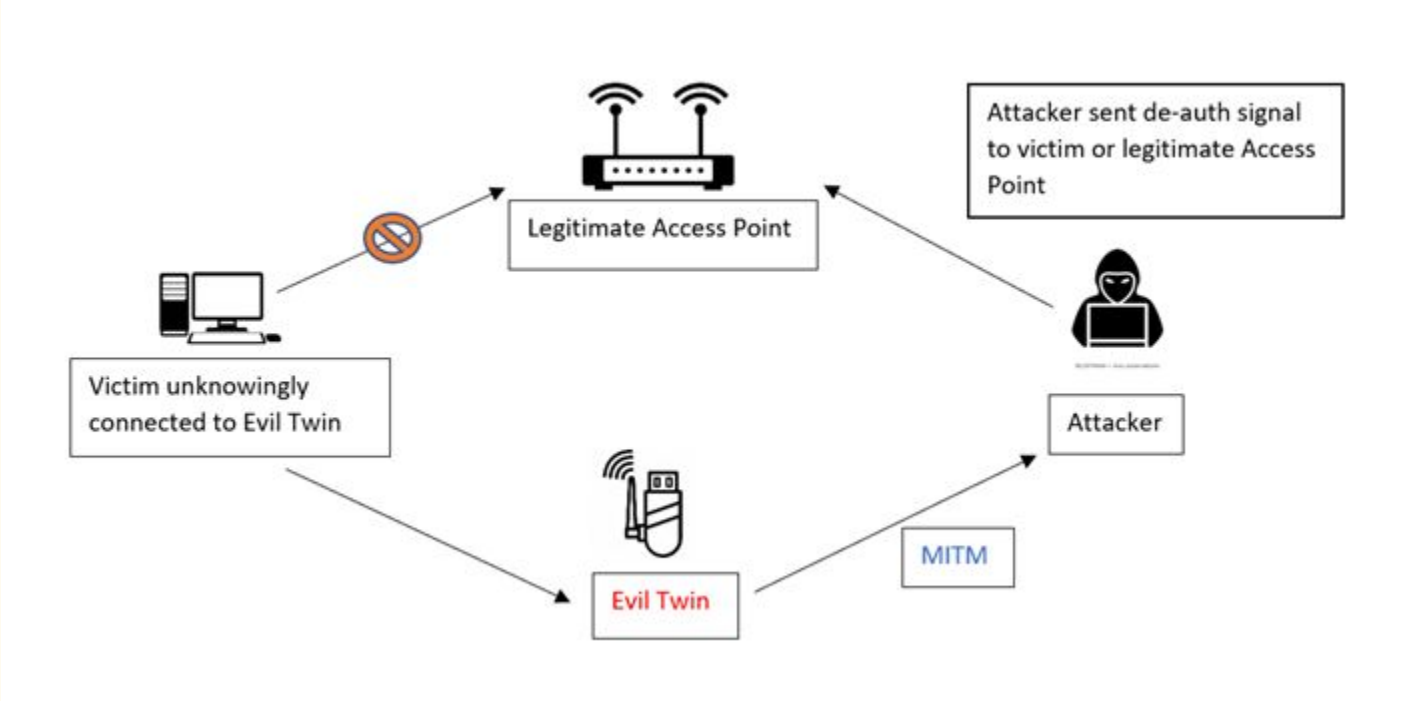
Evil Twin Attack

- Is Wi-Fi access point that pretends to be legitimate, but actually is set to eavesdrop on wireless communications

- It uses this fact that people always see the name or ESSID of wireless networks while using their phone or computers

- Using Social Engineering to try to force user to give the password

Evil Twin Attack Scenario



How To Perform Attack?

Steps :

1- Installing **Airgeddon** wireless attack framework

2- Change Wireless network adaptor to **monitor** mode, so can eavesdrop the network

3- Using **Captive portal** option in Airgeddon

A captive portal is something like the screen you see when connecting to an open network at a coffee shop, on a plane, or at a hotel and we'll be using that to our advantage to create a phishing page that looks like the router is updating

Steps :

4- Explore targets and gather the **Handshake** by **de-authentication** attack

5- SetUp **Phishing** page

6- Capture Network Credentials

With attack, victim will be kick of the network and will see fake authentication page. When victim joins fake network we get password and because of handshake we can detect incorrect password and wait to finally victim enter correct password

Defending Against Evil Twin

Know about attack and it’s signs

- If you abruptly lose the ability to connect to your trusted network and suddenly see an open wireless network with the same name, these are neither a coincidence nor a normal turn of event

- Never connect to an unknown wireless network pretending to be yours, especially one without encryption

- If you suspect your router is actually updating, turn off your Wi-Fi and plug into the router's Ethernet directly to see what the problem is

Thanks !

Network Security Course

Isfahan University Of Technology

Spring 2021

Any Question ?

You can find me at :

- amir.m.mansurian@gmail.com

documentations of this project :

- github.com/AmirMansurian/Hacking-Wireless-Networks