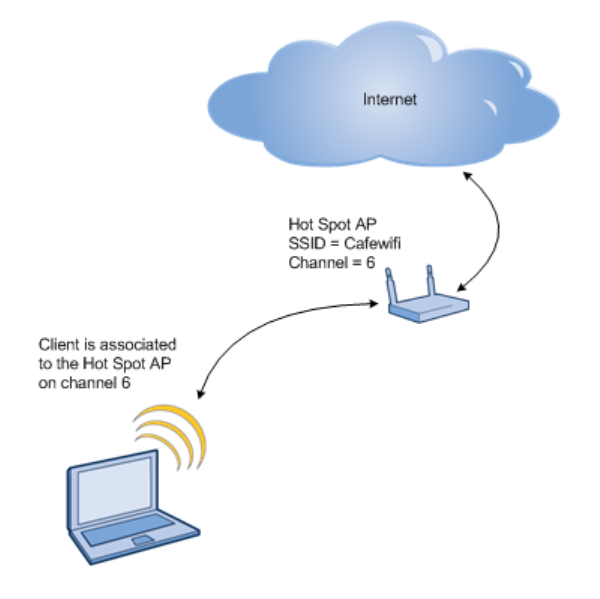
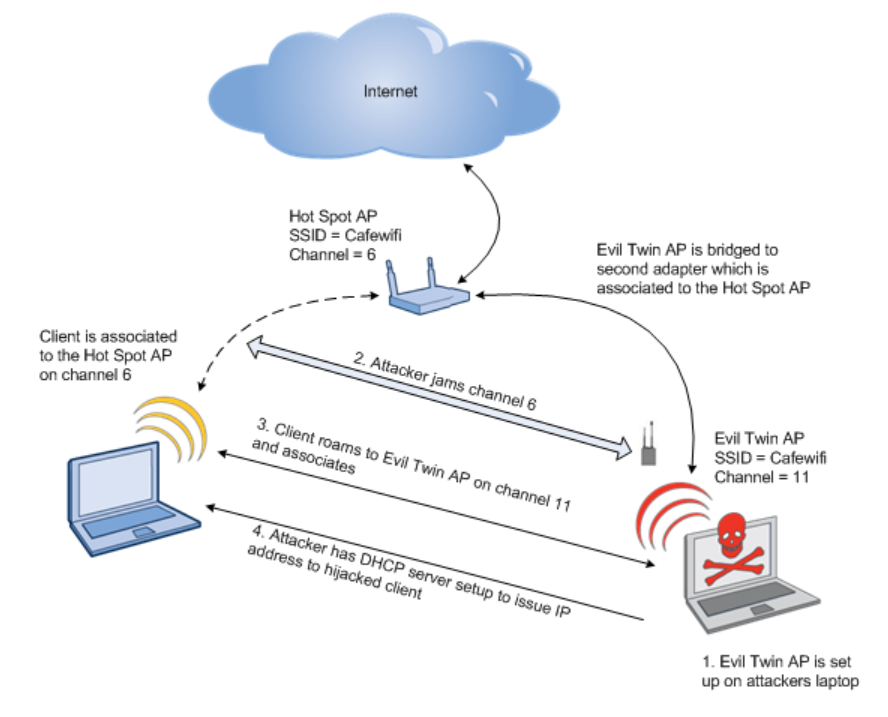
Evil Twin Attack  
By: Nathan Almaleh & Adam Lev-Ari   
Anywhere public Wi-Fi is available is an opportunity for an attacker to use that insecure hot spot to attack unsuspecting victims. One specific Wi-Fi hot spot attack called an “Evil Twin” access point can impersonate any genuine Wi-Fi hot spot. Attackers will make sure their evil twin AP is just like the free hot spot network, and users are then duped when connecting to an evil twin AP and the attacker can execute numerous attacks to take advantage of the unaware victim.



This diagram represents a regular internet connection.

  
  
  
  
  
  
  
  
  
  
  
As the user is using the free Wi-Fi the attacker is busy setting up the evil twin AP. The Attacker is not going to have a bunch of extra hardware, and you won’t see someone with a Netgear router or antennas sticking out everywhere to draw attention themselves. The attacker will more than likely have a laptop to launch the attack, and they could be in the same physical space or could be launching the attack from their vehicle in the parking lot.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
In this project we have created a tool that creates the evil twin attack from top to bottom .  
  
**Steps of our tool:**  
1.activating the interface card in a monitor mode (WLAN0MON)  
2.finding and displaying the information of the routers that the monitor has found .  
3.Selecting what router to attack by creating a new evil twin  
with the same SSID.  
4.Scanning for witch devices are connected to the router we have chosen by finding the mac address using sniffing tool.  
5.selecting what client to attack by sending multiple DE authentication packets .  
6.capturing the new handshake on the evil twin we have created  
  
**Summery :**  
This attack can be deadly and can be done so easily today in our modern world .  
By capturing the handshake we can use tools such as crack to find the password for the network and more tools for displaying the client interaction with the internet.  
  
**How to protect yourself from the evil twin attack**   
1.use a VPN connection   
2.dont set your device to automatically connect to the Wi-Fi you know .  
3.dont connect your self to open free Wi-Fi those are the most suspicious ones and easy to attack .  
4.use software like EvilAP\_Defender for detecting evil twins.  
5.coreate a tool that identify all the BSSID of the AP and connect your self to the only ones that have one BSSID and not multiple.