Don't “Locate Me”

Disclaimer:
This article is for educational purposes only. Check local laws before attempting. The author holds no responsible for the use of this information.

General Information:
As you may know, there is a new feature included in the Google maps 1.1.3 update for the Apple iPhone and iPod Touch; the “Locate Me” feature. The new feature is provided by another company called Skyhook Wireless (Http://www.skyhookwireless.com/). Skyhook's system is named “WPS” Wireless Positioning System and is for locating through a Wireless AP. "WPS" also is term coined by the Wi-Fi Alliance meaning "Wi-Fi Protected Setup". Skyhook achieves their locating features in a unique way because “WPS requires knowledge of the specific geographic location of individual access points ...This information is obtained by deploying hundreds of data specialists who scan and locate access points using proprietary scanning vehicles...“. Skyhook deploys approximately two hundred vehicles of wardrivers to scan, locate and then appends the information to a large reference database. The problem with the system, other than knowing someone has driven by your house or business and added your AP's information to a large database, is that a third party can then locate you with only your MAC address. I recently emailed Skyhook and inquired if there is a way for people to locate me through their service in response “...no, in no way can anyone track your location“. The second question was is it possible to have someone's AP's address removed from their database. They responded saying “...we[they] cannot remove individual access points...every access point by definition broadcasts a radio beacon ...The only way to stop an access point from broadcasting its presence is to unplug it....we don't actually identify the location of access points, just the signals that they create“. This information is particularly unsettling since Skyhook claims no other way to removing an AP's address from the database besides unplugging the access point.

This article will provide evidence contradicting both answers provided by Skyhook, as well as how someone with malicious intend could possibly discover your location.

Requirements:
Linux computer with a ethernet connection and wireless card capable of master mode.
iPhone/ iPod Touch or any other mobile device with the “locate me” feature.
Mac address of victim.
An isolated area where no access points have been located and added to Skyhook's reference Database.

Scripts :
skyhack.sh will create a bridge between the ethernet and wireless card to create an AP environment.
You can also use two wireless cards but the AP broadcasting must be unmarked by Skyhook. This would require editing the scripts.
delbr0.sh destroys the bridge, which returns your computer to normal.

```
#!/bin/sh
# Skyhack.sh 2008
wlanconfig ath0 destroy
ifconfig wifi0 down
macchanger wifi0 -m $1
wlanconfig ath0 create wlandev wifi0 wlanmode Master -bssid
iwconfig ath0 essid skyhack
iwconfig ath0 channel 6
ifconfig ath0 inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
route add default gw 192.168.1.1
ifconfig eth0 0.0.0.0 down
ifconfig ath0 0.0.0.0 down
brctl addbr br0
brctl addif br0 eth0
brctl addif br0 ath0
brctl stp br0 off
ifconfig br0 192.168.1.5
ifconfig eth0 up
ifconfig ath0 up
```

```
#!/bin/sh
# delbr0.sh part of skyhack 2008
ifconfig br0 down
brctl delif br0 eth0
brctl delif br0 ath0
brctl delbr br0
wlanconfig ath0 destroy
ifconfig wifi0 up
ifconfig wifi0 down
wlanconfig ath0 create wlandev wifi0 wlanmode Managed -bssid
```

Step 1: Gaining the MAC address of a victim
The process of acquiring a MAC address is beyond the scope of this article but I will provide some general ideas on how it may be accomplished. Wireless router packaging usually displays the MAC address on the outside of the box. Sales personnel at electronic stores could easily write down the MAC address and store that information until the product is sold. This is fairly useless because during the setup of a wireless router the MAC address can get cloned, which will then change the address, rendering the original information obsolete. Another way to acquire a MAC address is via social engineering. This is accomplished by conning an individual into divulging their MAC address. Google is another source that can be used to obtain MAC

addresses. Some people choose to post their MAC address while seeking help in a forum to solve a problem. Gaining access to a computer through a Trojan horse and running the command “arp -a” will also allow someone to obtain a MAC address on a Windows machine.

Step 2: Setting up your computer
The basic idea is to make your computer into an AP that spoof's the victims MAC. The way we do this is to bridge the ethernet cable and wireless card. The wireless card will then act as the access point of the spoofed victim. To run the bridging script run this command from the console “./skyhack.sh 00:00:00:00:00:00”. You need to changed the MAC to the 12 character MAC of the victim. Your connection is now bridged and the routers DHCP will hand out a IP to your mobile device when connected.

Step 3: Finding the approximate location
When you go to your Mobile device you should see the SSID "skyhack". Connect to "skyhack". To ensure that your connection is working properly check that your IP address is not a 169.254.0.0 address. Your web browser should then be used to load a website to guarantee that you are receiving internet traffic. If the above has worked, you are now ready to connect to Google Maps and use the "locate me" feature. Make certain there are no other AP's around, if there are, be sure that they are not in Skyhook's database as they can affect your results. By using the "locate me" feature you should now be able to see the victims approximate location within a 100m-200m diameter.

Step 4: Locating victims exact location
Use Google Map to give you driving directions to the approximate location given. To return your computer to normal function run "./delbr0.sh". This removes the bridge between your ethernet and wireless card, as well as returns your wireless card to managed or default mode. Now drive to the approximate location and scan the local area with your laptop or mobile device for the specific MAC address in question until the location pin pointed.

Prevention:
To prevent these types of security breaches keep your software patches up to date and use virus and malware scanners to prevent intrusion by others who may then acquire the MAC of your router. Also be wary of technical helpers over the phone or over the Internet who ask for your MAC address. A more definite way to prevent intrusion is to use the "Clone MAC" feature that can be found on most router configuration pages. This is primarily used to prevent the ISP from blocking internet access to your newly acquired hardware so that only your PC can access the internet. This tool can also be used to change the MAC address so that it will point intruders to nowhere or will point them to someplace completely different. Always check that the newly changed MAC address is not similar to a neighbor's. With Skyhook claiming it is not possible to remove single AP's from their Database this is the best method as long as you change the MAC often.

This method of locating has been tested with access points around my local area and also with a friend that lives almost 8000 km away. Please note that this "attack" is only as accurate as Skyhook's database.

As a side note these types of "attacks" could be used to inform friends about your home address. Instead of telling them the address is "2600 Robert St". You could say I am living at "00:00:00:00:00:00".

Notes:
The scripts provided in this article will not work out of the box with any wireless card or ethernet unless it uses ath0 and wifi0 and eth0. In most cases a simple change from ath0 to eth1 or wlan0 is all that is needed. Using different routers will also require different IP ranges. For example, Dlink would use 192.168.0.5 instead if 192.168.1.5.