Do you know what your phone is saying?

Did you know that your phone/connected device will automatically search for familiar Wi-Fi networks?

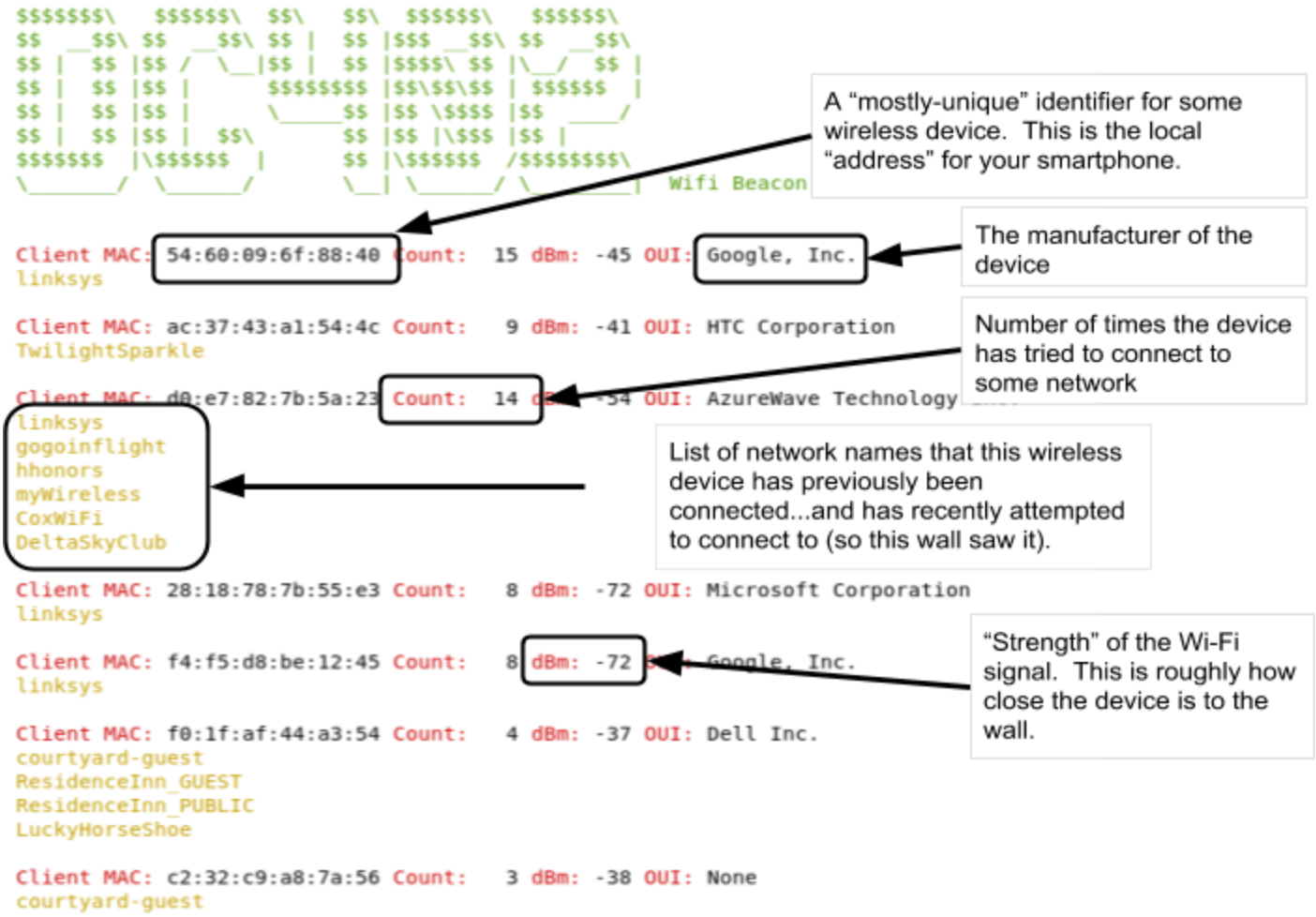
When Wi-Fi is enabled but not currently connected, your device will search for Wi-Fi networks it has previously used in the hopes of finding one it can connect to. Your device will transmit what is known as a *probe request*, which is your device asking if any of your remembered networks are nearby. These probe requests are sent "in the clear" and are not encrypted. Because your device needs to ask for specific network names, "Is free_airport_wifi here?" or "Is CoxWifi here?", anything listening can learn what networks you have used in the past. It is also possible for unsecured (or "open") Wi-Fi access points to be mimicked with minimal effort, so there is a chance someone could see your device ask, "Is free_airport_wifi here?" and they could respond in such a way that your device would automatically connect to the fake free_airport_wifi network. Typically, secured networks are much more difficult to mimic.

Here are some ways to manage what your phone is sending without your knowledge:

- Turn off Wi-Fi, Bluetooth, and NFC when you are not actively using them.
    - Whenever these services are turned on, they are extremely proactive in finding available connections, which means they are broadcasting data to anyone who may be listening.
- Remove old Wi-Fi connections from your devices.
    - The steps for Apple and Android devices are different, but a quick search for "Forget Wi-Fi networks <*type your phone model here*>" will likely bring up step by step instructions on what to do
- Delete old Bluetooth connections.
    - If you connect to a rental car, make sure you delete the connection from both your phone and the car. Data that is transferred often remains in the car even if the phone is not present.
- At home, secure your wireless networks with WPA2.
    - This requires configuration on your access point, typically clicking a checkbox to enable WPA2 and setting a password for your Wi-Fi network.
- If you would like to minimize the amount of identifiable information your devices may be broadcasting, ensure your home Wi-Fi network name does not contain identifying information you are not comfortable sharing, like "Bob Smiths House" for example.

Do you know what your phone is saying?

What's happening on the Wi-Fi display?



Our Wi-Fi wall displays recent connection attempts from the surrounding environment. It does this by monitoring the wireless activity and simply picking out the signals that Wi-Fi devices are emitting in attempts to connect to known networks. Networks to which each device attempts to connect are listed below the device searching for the networks, as well as some identifying information about the device itself.

Source code: https://github.com/ZonkSec/dc402-client-probe-dash