Deauthentication attack and other ‘wifi hacks’ using an ESP8266 module.

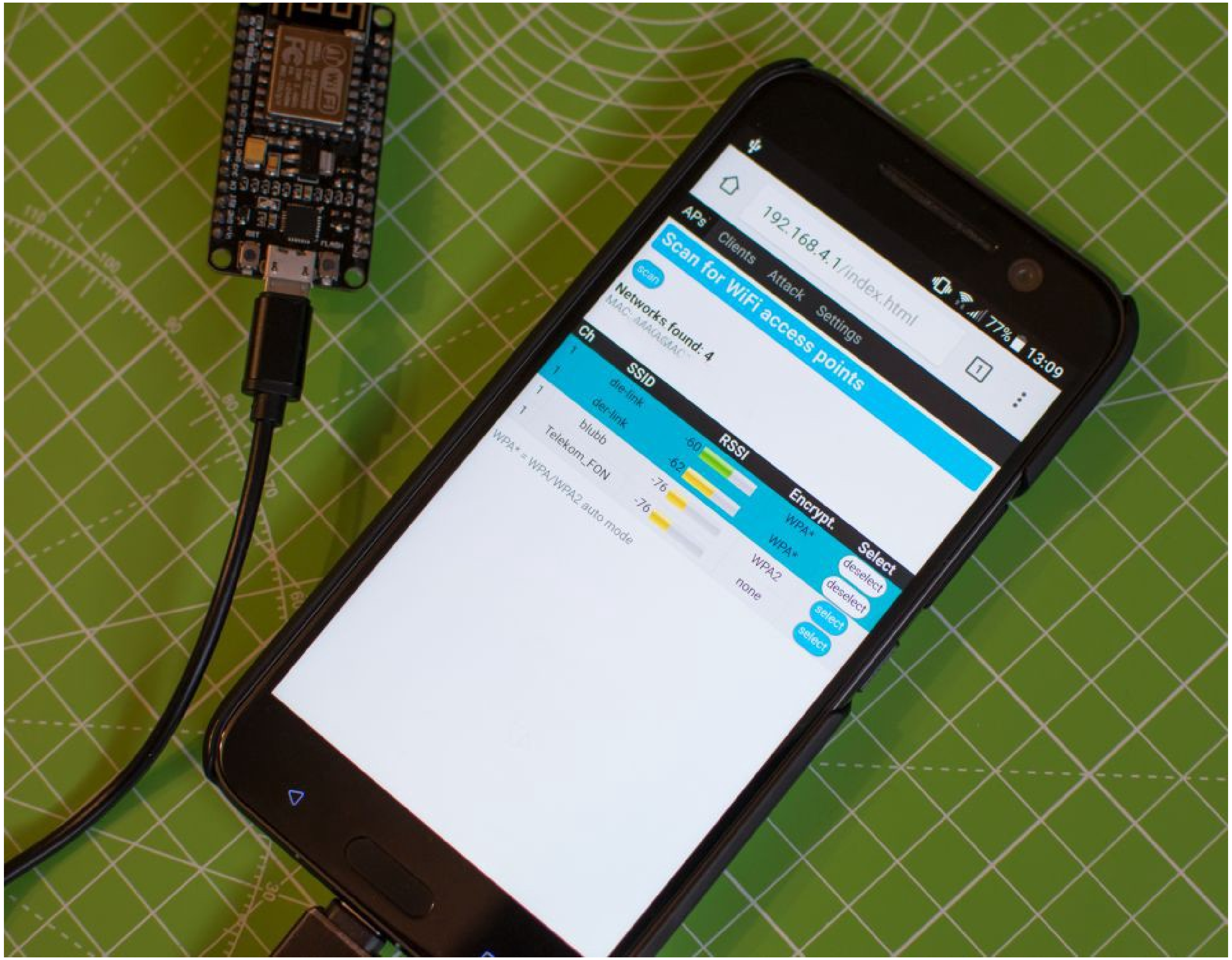
Tomas C. Follow

Jul 25, 2017 · 3 min read

As famed wifi hacker Samy Kamkar recently said we should move towards low-cost hacking/exploitation tools. NodeMCU is one of such tools, a LUA based firmware for the ESP8266 WiFi SOC under $5.

Now thanks to Spacehuhn you can assemble your own WiFi jammer (to be more correct wifi deauth attack tool) with an NodeMCU ESP8266. You select the wifi client you need to disengage from their wifi and begin the attack. For whatever length of time that the attack is running, any wifi will not work.

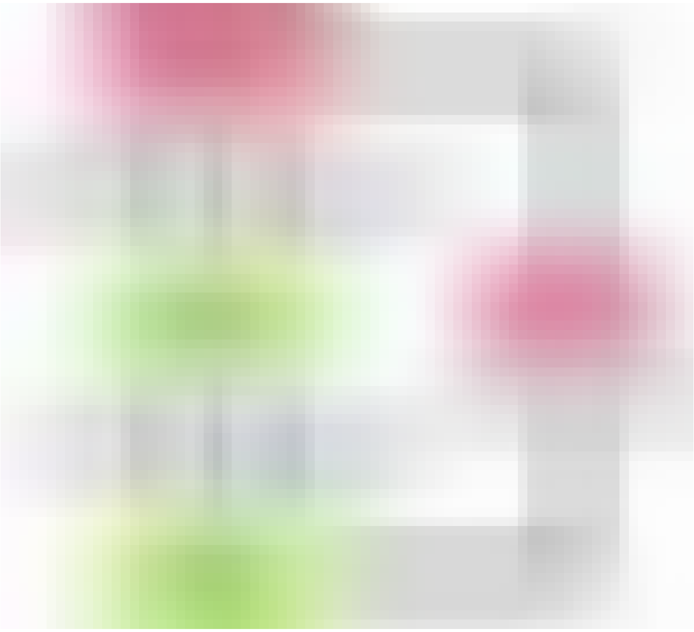
With a device like this you can disable the netflix streaming of your roommate, the wireless security cameras of the mall or your neighbor’s Internet of Things gadgets.



Ch	SSID	RSSI	Encrypt.	Select
1	die-link	-60	WPA*	deselect
1	der-link	-62	WPA*	deselect
1	blubb	-76	WPA2	select
1	Telekom_FON	-76	none	select

WPA* = WPA/WPA2 auto mode

The 802.11 WiFi protocol contains a deauthentication feature. It is utilized to detach customers from network. An attacker can send a station a deauthentication frame at any time, with a spoofed source address for the wireless access point. The protocol does not require any encryption for this frame, even when the session was established with. This vulnerability was addressed in 802.11w-2009 an approved amendment to the IEEE 802.11 standard to increase the security of its management frames, rarely supported is off course disabled by default.



Deauthentication Broadcast Attack

A decade ago, when strong, cheap magnets, bright LEDs, and small coin cell batteries were materials fresh to hacking, someone had a great idea: tape all these items up and throw them on bridges and overpasses. The LED throwie was born, and while we're sure the biggest installation of LED throwies looked cool, it's really just a small-scale environmental disaster. There are—and have been for a long time—expendable military radio jammers which are very small (artillery grenade or 'much less than backpack' small) and relatively cheap. These jammers can be used to knock out radio comm in a radius of several hundred meters. Emplacement is typically by hand or howitzer. Since then, the ESP8266 was created, and the world now has a tiny WiFi-enabled computer that's the size of a postage stamp and cost almost nothing.

Rand Druid battery powered, Compact ESP8266 based multi target De-Auth attack implementation.

While not recommended, it is an interesting example of the latest and cheapest technology that made a throwaway hacking tool possible; 10 years ago, a small wifi module this cheap would have been unthinkable.

Supported Devices: You can flash the code to every ESP8266. Depending on the module or development board, there might be differences in the stability and performance. The common ESP8266 512kb version won't have the full MAC vendor list and other features. NodeMCU ESP-12 based board which has 4mb flash and builtin USB port on it will work best.

Installation: Uploading the .bin files is the easiest way to get up and running.

https://github.com/spacehuhn/esp8266_deauther/releases

Always use the 1mb version , will work on 4mb, 32mb, etc. Unless you're sure that your ESP8266 only has 512kb flash memory.

Upload using the ESP8266 flash tool of your choice:
- nodemcu-flasher [Windows only]

- esptool-gui [Windows, MacOS]
- esptool [Windows, MacOS, Linux]

Power ESP8266 from OTG cable, powerbank, 2x AA battery. Scan for Wi-Fi networks and connect to *pwned*. The password is “deauther”.
Once connected, you can open up your browser and go to 192.168.4.1.