

JACK CLARK

DIY WIFI PINEAPPLE

\$WHOAMI

- 2nd Year Ethical Hacking
- iOS and MacOS Security
- @SynAckJack

WHAT IS A WIFI PINEAPPLE?

- Very powerful rogue AP
- Effective MITM attacks
- Great for reconnaissance

**WHO WANTS TO PAY FOR
SOMETHING THEY CAN MAKE FOR
LESS?**

DECISIONS DECISIONS

- Raspberry Pi ~ £30.00
- TP-Link WR703N ~ £28.00
- GL-AR150 ~ £24.00

GL-AR150

- Best bang for the buck
- Has a lot of features for example, dual ethernet ports and option for PoE, and can also run off of USB power
- Has very similar specs to the Nano

GL-AR150 SPECS

GL-AR150

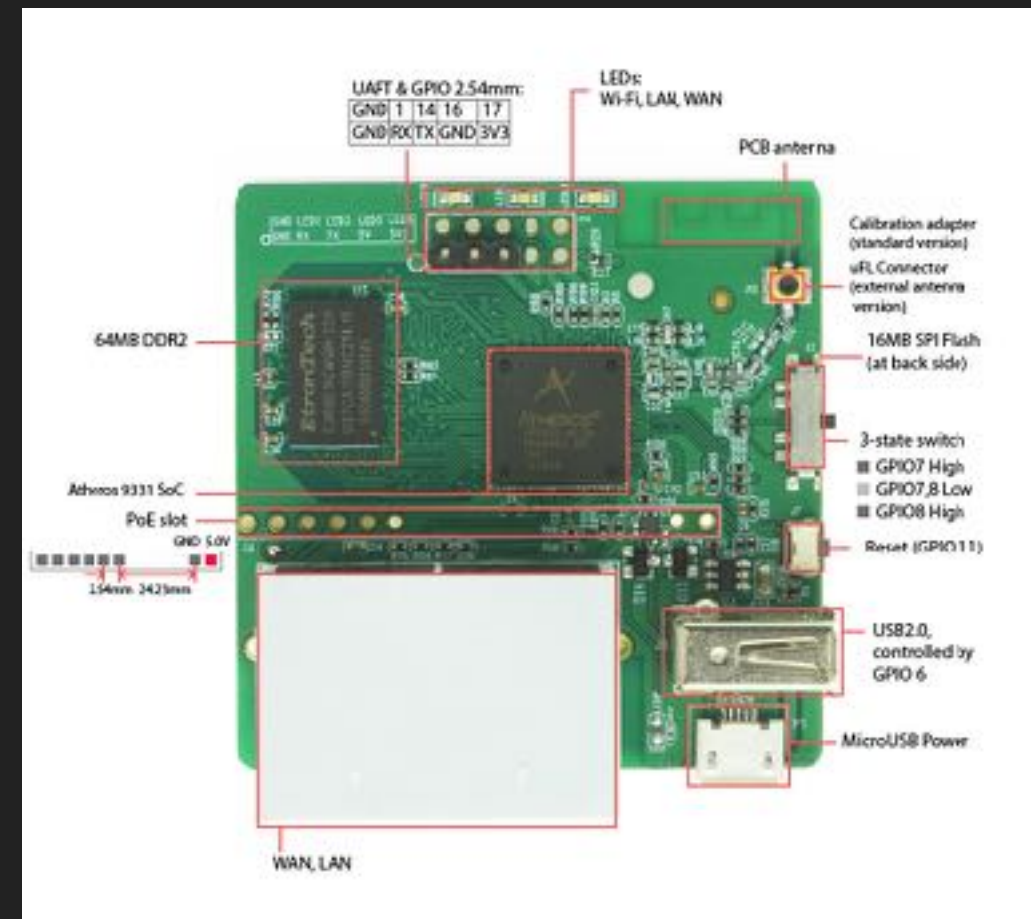
Atheros AR9331 SoC

64MB RAM

16MB on-board storage

2 ethernet ports, external antenna support

GPIO pins and UART built-in



SO HOW?

- Requires Wifi Pineapple firmware and OpenWRT patch for AR150
 - Extract Wifi Pineapple firmware using binwalk
 - Copy contents of squashfs/root folder extracted in previous step to OpenWRT Patch Files folder
 - Build OpenWRT
 - Flash firmware to AR150

**WELL THATS A BIT OF A
LONG WAY TO DO IT...**

JUST DOWNLOAD PRE- COMPILED FIRMWARE

PLENTY OF REPOSITORIES ON GITHUB

**AND IT JUST
WORKS...KINDA**

**THERE ARE A FEW DRAWBACKS AND
ISSUES**

THE DOWNSIDES

- Internet sharing between a PC/laptop isn't the easiest
- If you don't have a USB WiFi adapter, it won't quite work either
- If you try to update the firmware through the UI then it will brick the device as well

PUB?

YOU CAN ASK ANY QUESTIONS THERE