Notes of DIY Pineapple router

ABOUT PINEAPPLE ROUTER HARDWARE AND SOFTWARE

Wi-fi Pineapple is a special wireless tool developed by Hak5. It looks like a typical wifi router, but it is designed to do penetration testing, network auditing, and other types of testing. It can also be used to perform man-in-the-middle attack, credential harvesting and other pen testing tasks through simulated open or cloned networks. It costs around 100-240 depending on the router type and features.

SOFTWARE:

After doing research we found out that pineapple router uses **OpenWRT**, which is a Linux based operating system designed for embedded devices. It also has a graphical UI and comes with pre-installed tools for pen testing. Pineapple router uses **Mips_24Kc** architecture. Mips 24Kc is 32-bit Reduced Instruction Set Computing (RISC) architecture that comes from the MIPS family. It is often used I different routers, gateways, and embedded system. Mips 24Kc is compatible with OpenWRT.

- OpenWRT OS: https://openwrt.org/start
- Mips_24Kc architecture catalog: https://s3-eu-west-1.amazonaws.com/downloads-mips/documents/MD00346-2B-24K-DTS-04.00.pdf

Pineapple router uses different Pineapple software for their products **Nano**, **Tetra**, **MK5**, **MK4**. We are probably going to use **Pineapple Tetra**.

- Pineapple software link: https://www.wifipineapple.com/downloads#tetra

HARDWARE:

1. ROUTER WE ARE CONCISDERING TO IMPLEMENT PINEAPPLE SOFTWARE

So, after considering all the needed specs we decided we would implement the Pineapple Tetra to **Tp-link Archer C7 AC1750** router.

- Tp-link Archer C7 AC1750 official page: https://www.tp-link.com/se/home-networking/wifi-router/archer-c7/
- Specs list from OpenWRT page: https://openwrt.org/toh/hwdata/tp-link/tp-link_archer_c7_ac1750_v2.0
- Other potential router lists:
    - https://openwrt.org/docs/techref/instructionset/mips_24kc
    - https://gitlab.com/xchwarze/wifi-pineapple-cloner-builds

2. USB flash drive
3. Power bank

IMPLEMENTING SOFTWARE TO HARDWARE:

- After you have your TP-Link Archer C7 router ready, you also need to have a USB WiFi adapter, MicroSD card, ethernet cable and your own computer (preferably macOS or Linux based) with you.

- Start by downloading the OpenWrt firmware and then install it to the router. Instructions for this can be found on the OpenWrt website https://openwrt.org/docs/guide-quick-start/factory_installation

- Connect the router to your computer with the ethernet cable. A prompt should come up that helps you setup and configure the basic settings and also make sure that the router works fine. Now you want to install the WiFi pineapple software to the router. For this, you will first need to go to the github repository “wifi-pineapple-cloner" https://github.com/xchwarze/wifi-pineapple-cloner/
- on your computer. Navigate the repository and make sure that you find and download the right WiFi Pineapple software file for your router (the github repository has different download links for all the supported devices).

- Now you can copy the downloaded file to the router’s file system. You can use scp (secure copy) to do this. Finally, ssh to the router and run the file. This will take a couple of minutes, but after it’s done, you should see a new available WiFi connection called Pineapple_”something”.

- Connect your computer to that network and write to your browser: 172.16.42.1:1471 (The page that opens will let you make the final modifications to the pineapple router). If the IP address does not work, check the wifi-pineapple-cloner github page, in case the IP is something different.

COMPLICATIONS WE MIGHT FACE:

- Issues from the router are expected because the model is now deprecated, and issues can arise during the project.
- Compatibility between software and hardware may arise since it has not been tested before.
- Ethical issues might occur because this is a hacking device.
- Power bank might not provide the required power, and the portability of the device can be affected.
- The processing power of the router is lower as128MB for RAM. This might be an issue when scanning larger networks which means larger payloads.

EXTRA FEATURES:

- Although it's not planned in primary design, an alert can be generated when the battery level of the power bank goes down after a certain level.
- If the device is planned to be used for educational purposes, an automated message can be sent to users mentioning that user has been connected to malicious network with some information about how to avoid similar kind of situation.

Group members:

1. Rafiqul Talukder - Y53019674
2. Valtteri Suominen - Y48522508
3. Piyumi Weebadu Arachchige - 2304801