Hardware Hacking

This challenge is one part of a 5 flag challenge. It will feature multiple different techniques and common security blunders. All the challenges will require the Secret Vault board to solve.

Purpose of hardware

Think of the hardware as something similar to a hardware crypto wallet. It is supposed to keep your crypto safe, or in our case, our pin codes and flags.

But this secret vault has some common hardware security issues that we are going to try to exploit.

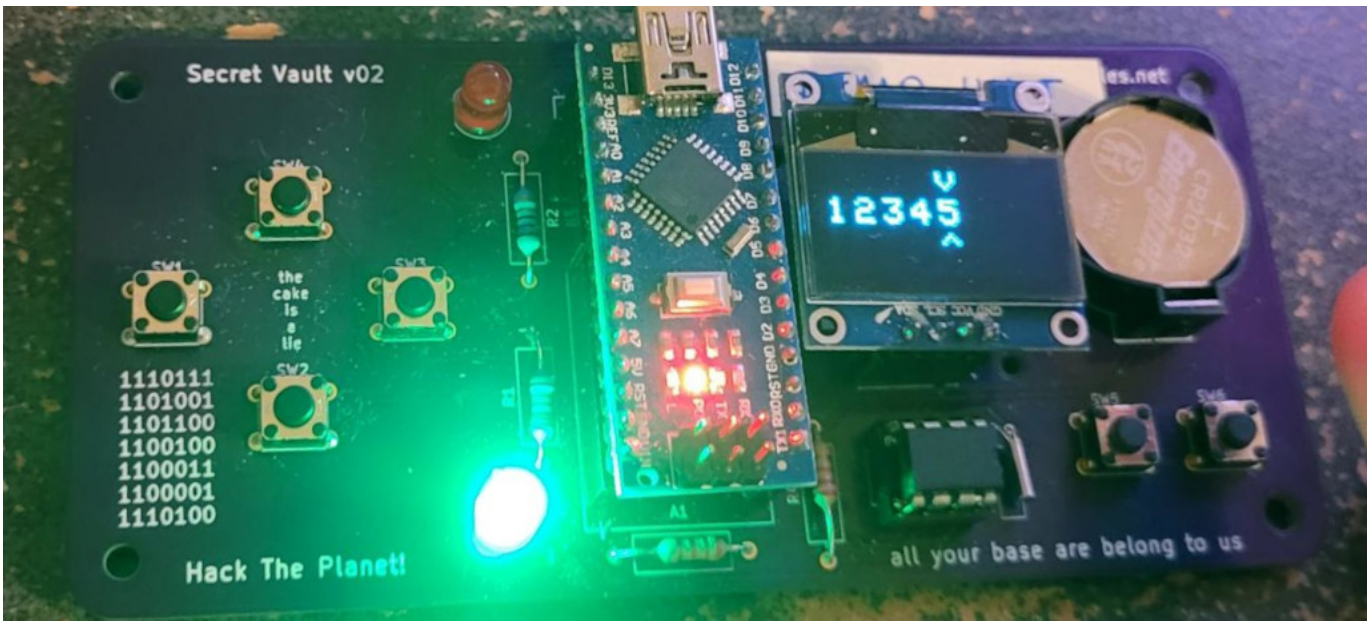
The vault is normally locked, but if you enter in the secret pin code, it will unlock, and then you can read secrets, and play the snake game. The attached files are challenge description document, hardware documentation, and a sanitized copy (no flags included) version of the source code.

Demo Board

One of the boards is the demo unit. The only real flag it has is for challenge 5, the rest of the flags in it are sample flags.

Firmware Mode	Demo Pin
Ver 1.0	12345
Ver 1.1	23456
Ver 1.2	34567
Ver 1.3	45678

Use the demo board to help you identify some of the flaws, how the board works, and how to get it to show you the flags.



Challenge 1 - Ver 1.0 - Flag via Serial CLI

Embedded hardware devices almost always have a serial interface for information and troubleshooting purposes. A serial port may just have logging messages, but they often will have interactive shells. If these interfaces aren't secured, they can reveal a tremendous amount of information to a hacker.

For this challenge, you should connect your computer to the serial interface (which on this board is on the USB interface).

For this type of work, I usually install a program called picocom on Linux, or Putty on Windows. For Linux, I usually like to add my user to the dialout group and then reboot for change to propogate into the window manager:

```
sudo adduser username dialout
sudo reboot
```

Adding the user to the dialout group will let you open the serial port without invoking the sudo command to elevate privleges.

Monitor the serial port while you use the board and get the hang of how it works. There is some debug code running on this version of firmware that shouldn't be running, that you can exploit to get the flag.

Challenge 2 - Ver 1.1 - Brute force via serial port

To access this challenge, you will have to need to first upgrade the firmware version that is running on the challenge board to V1.1. The source code for the software will probably be of great help in figuring out how that is done.

The debug code that gave away the flag on the last challenge has been removed now. You can unlock the device by brute forcing the pin code. The serial interface provides a command to unlock the device, and the pin is a max of 5 digits long, which won't take long for a computer to brute force.

Challenge 3 - Ver 1.2 - Brute force via buttons

With this firmware version, the serial interface now has some brute force protection mechanisms in place. But that is not the only way to brute force the pin.

Can you exploit the hardware using some of your own hardware devices to brute force the pin code still?

You will need an Arduino kit to complete this challenge.

Challenge 4 - Ver 1.3 - No brute forcing

All interfaces for entering the pin have been protected against brute force attacks. But if we look at the datasheet for the DS1207 module and understand how the hardware works, we can monitor some of the signal on the board to see it transfer the secrets that protect the pin.

You will need an Analog Discovery to complete this challenge.

Challenge 5 - Any version - Snake Game

This challenge works on any board. There is a flag that gets printed if you set a new high score in the snake game. Can you get the high score flag?