TP Attaques matérielles et sécurisation

Dump de mémoire SPI

TLS-SEC, 2024-2025

12 décembre 2024

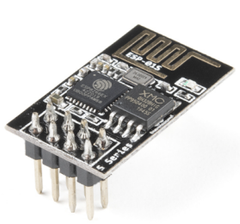
Objectifs

Ce TP a pour but d'apprendre à lire et patcher un firmware en accédant directement à la mémoire. Ce TP couvre les aspects suivants :

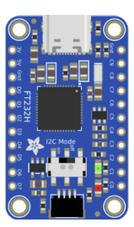
- Prise en main du matériel.
- Rétro-ingénierie d'un PCB (Printed Circuit Board) simple.
- Probing/sniff des communications sur le PCB.
- Dump et analyse d'un firmware.
- Patch et écriture du programme.

1 Prise en main du matériel

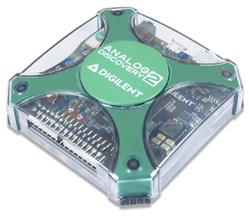
1.1 Présentation des équipements



(a) Module ESP-01S



(b) Module FTDI 232H



(c) Analyseur Digilent Analog Discovery 2

Vous disposez du matériel suivant :

- Une cible basée sur un module WiFi ESP-01S `https://cdn.sparkfun.com/assets/f/e/5/6/f/ESP8266ModuleV2.pdf`)
- Un analyseur Digilent Analog Discovery 2 `https://digilent.com/reference/test-and-measurement/analog-discovery-2/start`

- Un module FTDI FT232H `https://learn.adafruit.com/circuitpython-on-any-computer-with-ft232h/pinouts`
- Un set de 10 fils Dupont

La cible est un module WiFi/Bluetooth très utilisé dans le monde de l'IoT. Dans le cadre de cette étude, le module expose un serveur web (`http://192.168.4.22:8080`) via le WiFi (mode Access Point). Cependant, vous ne disposez pas des identifiants de connexion au point d'accès.

L'Analog Discovery est un périphérique USB multifonction permettant (entre autre) de :

- Capturer des signaux logiques (16ch logic analyzer)
- Générer des signaux logiques (16ch pattern generator)
- Capturer des signaux analogiques (2ch oscilloscope)
- Générer des signaux analogiques (2ch arbitrary waveform generator)
- Générer une tension d'alimentation stabilisée (2ch programmable power supply)

Cet instrument permettra d'alimenter la cible (en 3.3V), et de capturer des signaux logiques. On l'utilise avec le logiciel "waveforms".

Le module FT232H permet de s'interfacer avec des bus tels que le l'UART, le SPI, l'I2C, le JTAG. Dans le cadre de ce TP, on l'utilisera avec le logiciel open-source "flashrom" (`https://github.com/flashrom/flashrom`) :

```
flashrom -p ft2232_spi:type=232H,serial=1234567 ...
```

Note : le paramètre "serial" est nécessaire en cas de conflit (ex. avec l'analog discovery). Pour retrouver la valeur :

```
lsusb -v -d 0403:6014 2>/dev/null | grep -B2 iSerial
  iManufacturer           1 FTDI
  iProduct                2 C232HM-DDHSL-0
  iSerial                 3 1234567
```

1.2 Validation du matériel

1. Exécutez le script `/mnt/gei/TP_FLASH_SPI/setup.sh` dans un terminaal afin de préparer l'environnement.
2. Connectez l'analyseur Digilent, et ouvrez l'application "waveforms".
3. Vérifiez que le périphérique est correctement reconnu (Settings -> Device Manager : "Analog Discovery 2" sélectionné)
4. Configurez le périphérique (Settings -> Device Manager) en sélectionnez la 4e ligne (16x16k de mémoire "Logic")
5. Connectez le Module FT232H
6. Exécutez la commande


```
flashrom -p ft2232_spi:type=232H,serial=1234567
```

7. Validez la version de flashrom (flashrom v1.2-1144) et la communication avec le module FTDI (Message attendu : "No EEPROM/flash device found").
8. Exécutez la commande "esptool.py version" et validez la version (v4.4). (si besoin, téléchargez `https://github.com/espressif/esptool`)

1.3 Démarrage de la cible

1. Connectez le signal de référence (fil noir) entre l'Analog Discovery et la cible (pin "GND")
2. Connectez le signal d'alimentation positive (V+) à la cible (pin "3V3")
3. Ouvrez le logiciel "wafeforms"
4. Cliquez sur "Supplies" et réglez la tension positive (V+) sur "3.3V"
5. **Faites valider le montage avant de continuer**
6. Pour plus d'information référez-vous au manuel.
7. Identifiez le SSID correspondant à votre cible (cf étiquette sur le module ESP). 18667176

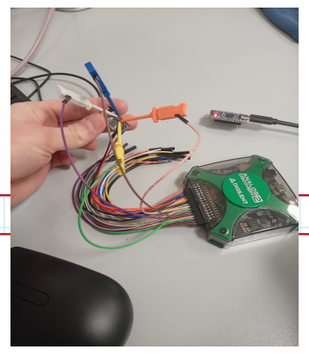
2 Rétro-ingénierie du circuit imprimé

Énumération passive :

1. Identifiez les composants présents sur le module et récupérez les documents constructeurs publics des deux circuits intégrés.
2. Quel est le composant principal (où s'exécute le programme) ? Quelle est l'architecture du CPU ? Quelle est sa fréquence max ? ~> ARM, 128MHz + coprocesseur RISC-V 128MHz
3. Question optionnelle : Donnez la cartographie mémoire du composant principal ?
4. Identifiez les composants comportant de la mémoire ? Pour chaque type de mémoire, indiquez leur taille, leur type (ROM, RAM, Flash, EEPROM, ...). Indiquez une méthode pour lire et/ou programmer ces mémoires.
5. Où se trouve le firmware ? dans la mémoire
6. Le SoC fournit-il des mécanismes de sécurité pour protéger le firmware (chiffrement, signature, verrouillage des interfaces de débogage.....)

Énumération active : Observer les accès mémoires lors du démarrage du composant à l'aide d'un analyseur logique

1. Expliquez le rôle des signaux du bus SPI. Qui est le maître ? transmette data
2. Repérez les signaux sur la mémoire
3. Quelle est le format des trames (lecture/écriture) ?



4. Réalisez le montage pour capturer les échanges entre les deux circuits intégrés avec l'analyseur logique. **Faites valider le montage avant d'allumer !**
5. **Après avoir fait valider le montage**, capturez au démarrage du composant avec l'analyseur logique (Vue "Logic", Mode Record, Sampling rate 50MHz, 256k Samples, Trigger sur "CS"). Attention : Vérifiez la taille du buffer "Logic" (16x16k) dans Settings/Device Manager
6. Quelle est la première commande ? Que répond le composant ?
7. Quelle est la première adresse lue ? Donnez la taille et le contenu de la première lecture (**0.5 point bonus**)

3 Exploitation

L'objectif de cette partie est de récupérer le mot de passe de connexion qui se trouve dans la mémoire.

1. Après avoir débranché l'analyseur logique, connectez le module FT232H à la mémoire (débranchez aussi l'USB pendant l'opération)
2. Que faut-il faire pour permettre de lire la mémoire sans être gêné par le contrôleur ?
3. Après avoir fait valider le montage, récupérez le firmware avec l'utilitaire flashrom.
4. Analysez le binaire avec esptool.py. Quel est le point d'entrée ?
5. Récupérez le mot de passe du point d'accès Wi-Fi et connectez-vous (**0.5 point bonus**)
6. L'ESP expose une interface web. Connectez-vous. Pouvez-vous accéder à l'interface d'administration ? http://192.168.4.22:8080

4 Escalade de privilège

L'objectif de cette partie est de vous connecter à l'interface d'administration.

7. Retrouvez les identifiants dans le binaire. Le mot de passe est-il en clair ? Que pourrait être l'algorithme ? Comment accéder à l'interface d'administration ? sha256
8. Connectez l'interface série au Module FT232H ; et utilisez l'utilitaire de console favori/-disponible (screen, minicom, etc...). Le baudrate est 115200 baud/s.
9. Affichez les messages de débogage sur la console. Comment est construit le hash ?
10. Comment peut-on accéder à l'interface d'administration ?
11. Patchez le firmware.
12. Après avoir reconnecté le module FT232H à la mémoire, reprogrammez la mémoire.
13. Accédez à l'interface d'administration. Quelle est le flag ? (**1 point bonus**)