Reverse etiqueteuse supvan E10

- Etiqueteuse Supvan E10

Etiqueteuse Supvan E10

Bonjour :)

Il y a quelque temps, j'ai acheté une simple étiqueteuse Bluetooth sur Amazon et elle fonctionne avec une application Android nommée "Katasymbol".

Cette application limite grandement ce qu'il est possible de faire avec l'imprimante, par exemple, il n'est pas possible de répéter x fois un texte (pour faire une étiquette autour d'un câble par exemple).

Je me suis donc lancé dans le reverse de cette application mobile ainsi que la communication Bluetooth.

Exploration

J'ai d'abord commencé par récupérer l'APK et le lire avec Jadx, c'est un outil permettant de décompiler le byte code java.

Je cherche notamment ou sont envoyés les paquets Bluetooth pour ensuite remonter aux fonctions liées à l'affichage, l'impression, etc.

image.png

La fonction sendCmdStartTrans contient un tableau bArr2 qui correspond à un paquet Bluetooth (RFcomm) qui est une simple liaison série en Bluetooth.
Les nombres dans le tableau sont la représentation des bytes.

J'ai maintenant voulu analyser les trames Bluetooth faites par mon téléphone quand il communique avec l'étiqueteuse.

En utilisant un téléphone rooté et avec la partie Bluetooth HCI snoop activé dans le mode développeur, il faut taper cette commande en ADB :

```
adb shell su -c "'nc -s 127.0.0.1 -p 8872 -L system/bin/tail -f -c +0
/data/log/bt/btsnoop_hci.log' &"
```

Cela permet ensuite de voir les trames dans Wireshark.

image.png

Grace au code de l'application mobile ainsi que des trames bluetooth, j'ai commencé à reproduire certaines fonctions via un petit programme python (récupération du nom de l'appareil, du

firmware, etc).

Sur le dépôt Git.

J'ai fait des fonctions qui permettent de convertir une trame en hexadécimal vers des bytes puis vers la représentation des bytes en nombres.