DVID

WOCSA

Worlwide Open Cyber Security Association

CYBLEX Consulting

Cyber IoT,
The hacker way

dvid.eu

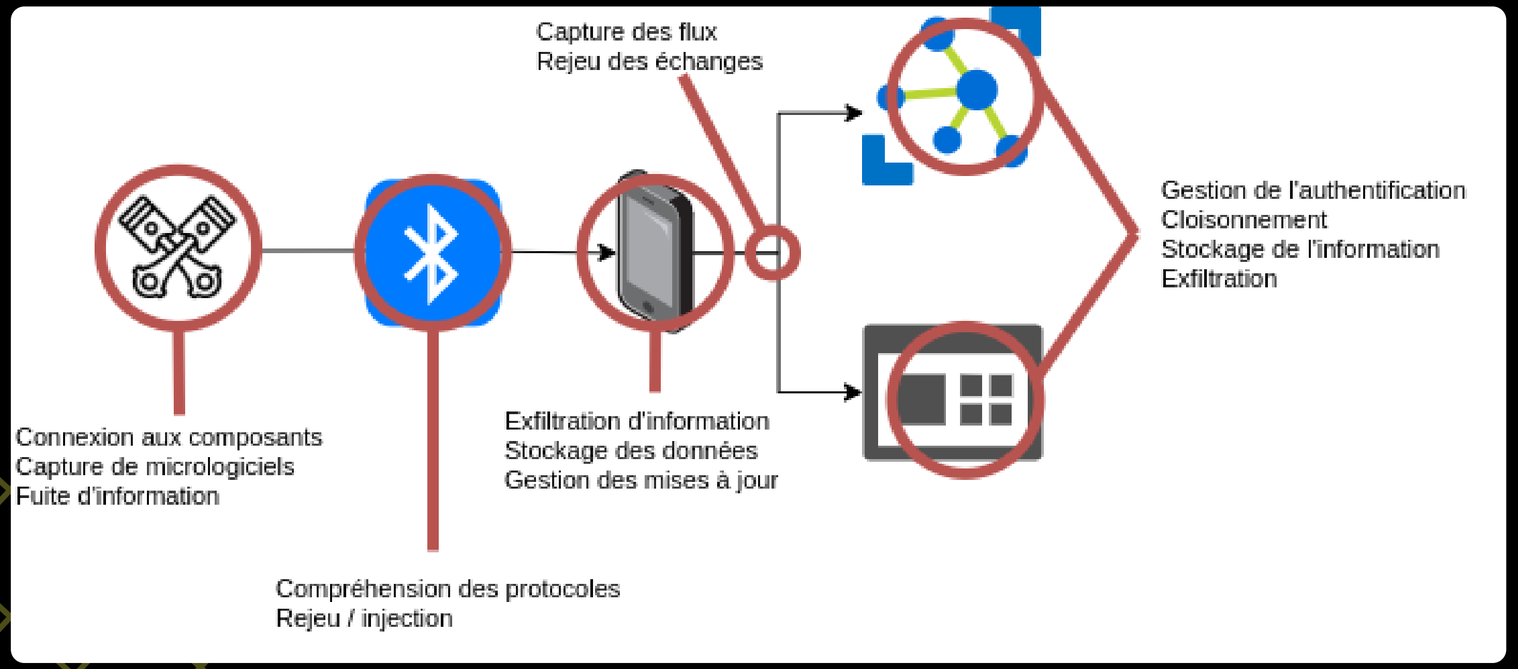
REAL FIELD ACTUALITY

Pacemarker (2017)

LG SmartThinQ (2016)

Volkswagen (2015)

THE ECOSYSTEM



30%
of hardware

20%
of cloud computing

20%
of data transport

30%
of only data

En pratique

- Ports de debug accessibles
- Lecture mémoire depuis le bootloader
- Reconstruction du micrologiciel
- Extract des binaires
- Exploitation à distance

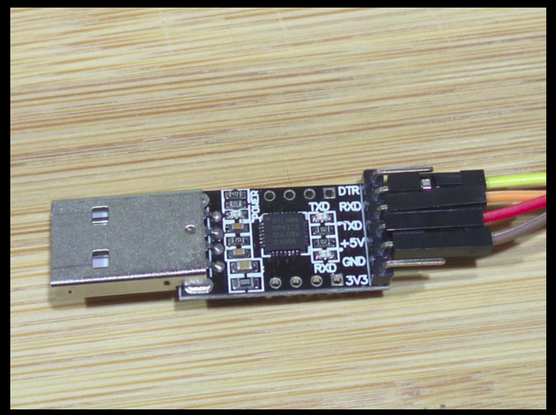
```
[ ] crc32 (NEW)
[*] md (NEW)
[*] memcmp (NEW)
[*] memcpy (NEW)
[*] memset (NEW)
[ ] memtest (NEW)
[ ] memtester (NEW)
[ ] memory modify (mm) (NEW)
[*] mw (NEW)
```

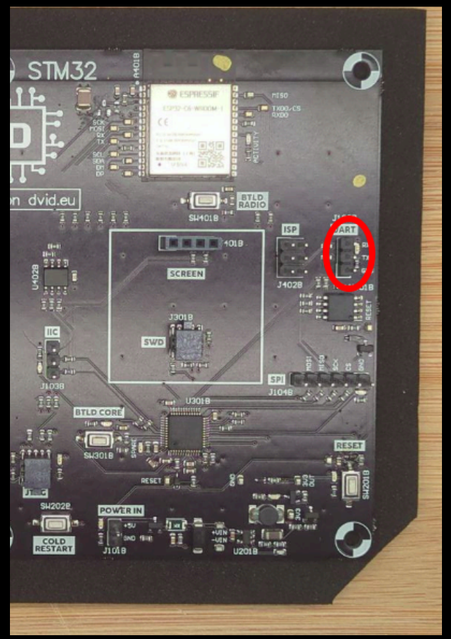
```
=> md.b 0x4000000 0x50
04000000: de ad be ef de
04000010: de ad be ef de
04000020: de ad be ef de
04000030: de ad be ef de
04000040: de ad be ef de
=>
```

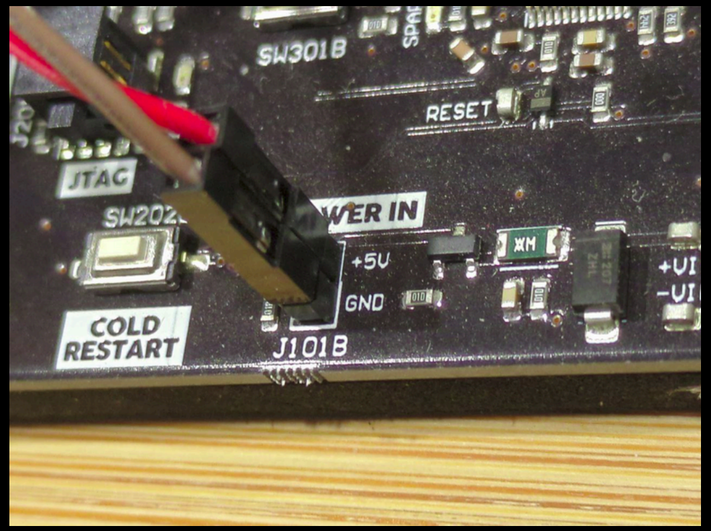
A vous de jouer

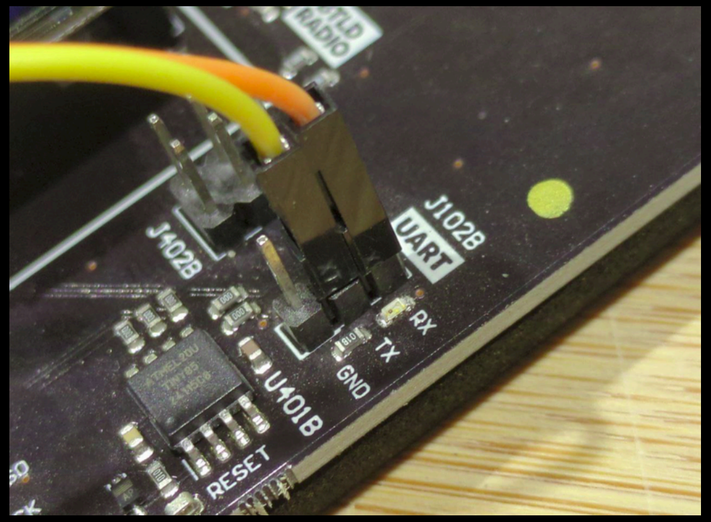
This workshop will focus on STM32 side.

Objective : Take the UART dongle and wiring correctly

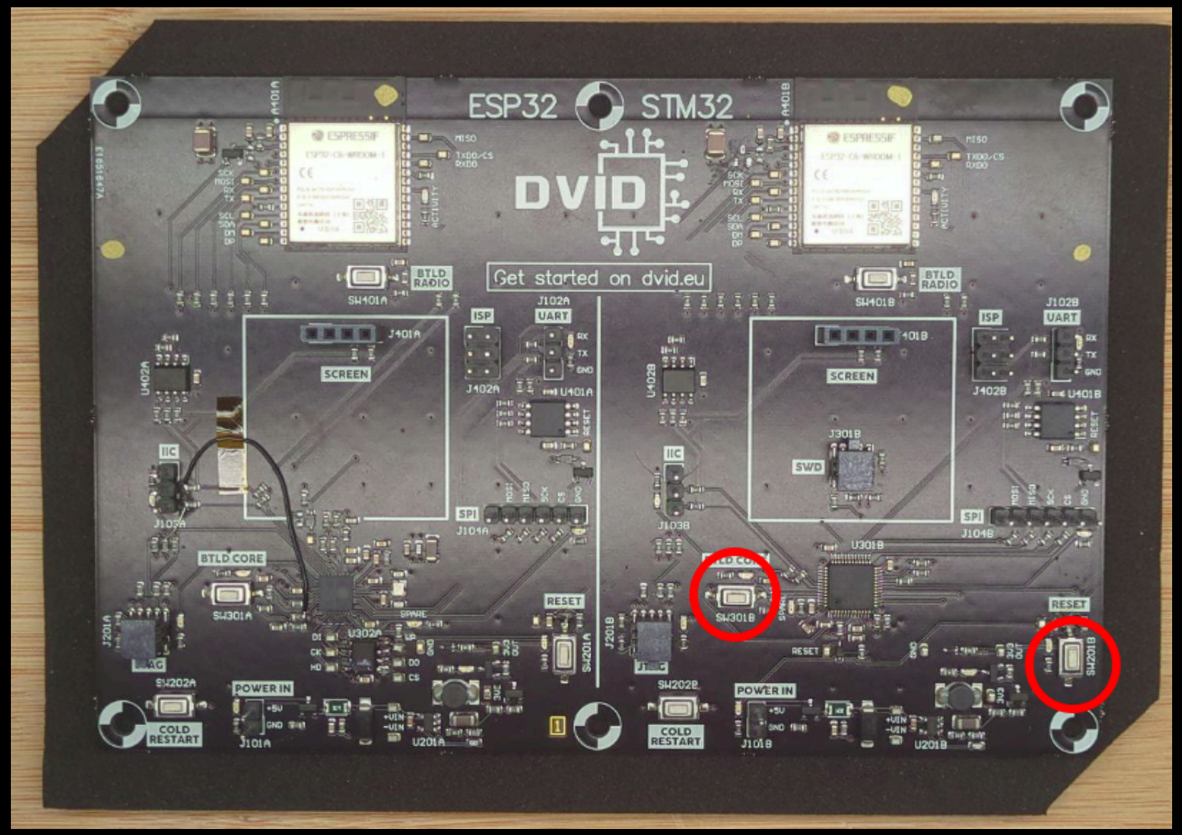








A vous de jouer (read flash)



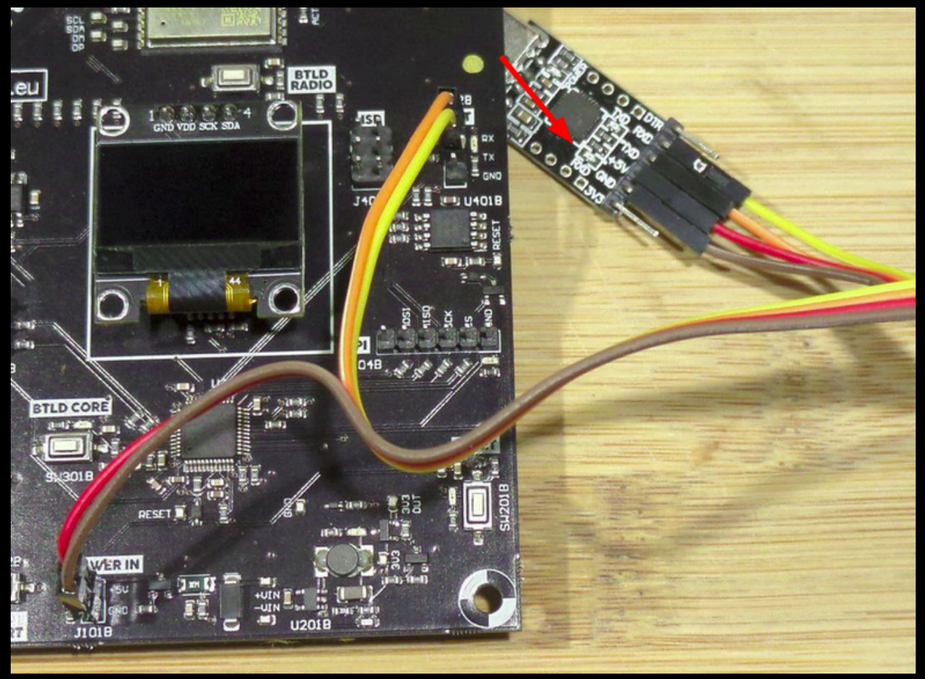
HOLD BTLDCORE
HOLD & RELEASE RESET

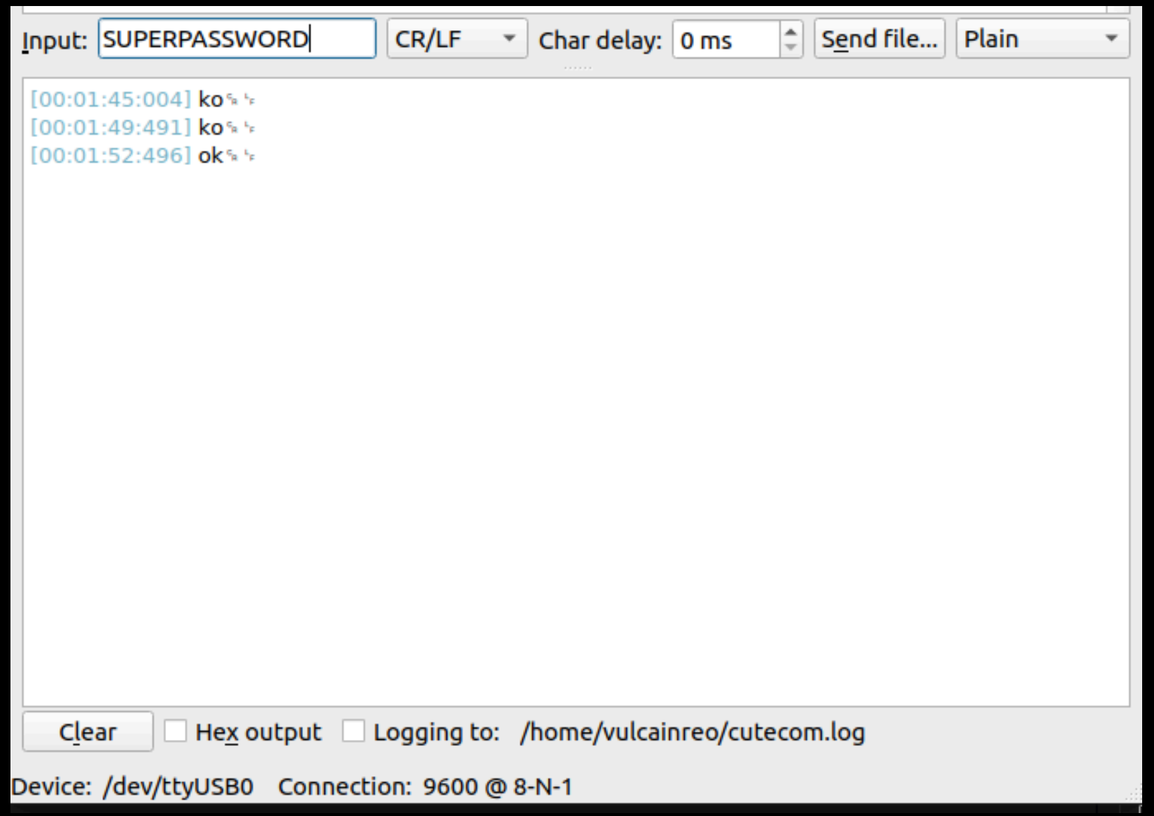
strings test.bin | grep -i pass

Pass from UART ?
SUPERPASSWORD

Arduino_STM32/tools/linux64/stm32flash/stm32flash -b 115200 -r test.bin /dev/ttyUSB0

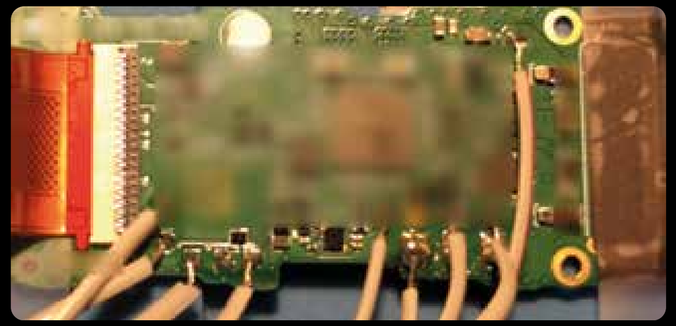
A vous de jouer (UART password)





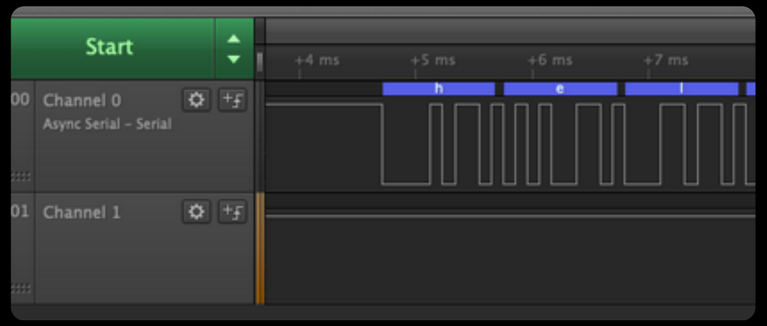
https://packages.debian.org/fr/sid/amd64/cutecom

Dans la réalité



Soldering on PCB

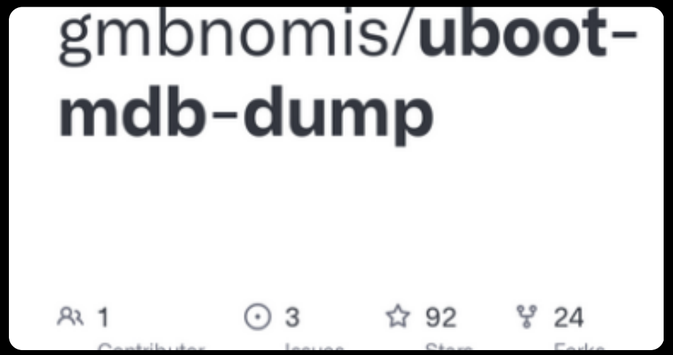
UART



Probing of signals

```
=> md.b 0x4000000 0x50
04000000: de ad be ef de
04000010: de ad be ef de
04000020: de ad be ef de
04000030: de ad be ef de
04000040: de ad be ef de
=>
```

Memory display



Firmware recovery

Firmware emulation

```
memset(acStack152,0x0200);
sprintf(acStrack152,"echo input:%s>/tmp",pcVar1);
system(acStrack152)
```

Firmware disassembly

En pratique

- Serveur MQTT accessible sans authentification
- Possibilité de souscrire à des jokers (#)
- Accès aux informations des autres clients
- Accès illégtime au SYS
- Accès à des données RGPD

DEMO

- device
  - 269054958815780
    - batt = 73
    - state = on
  - 167024525700489
    - batt = 73
    - state = on

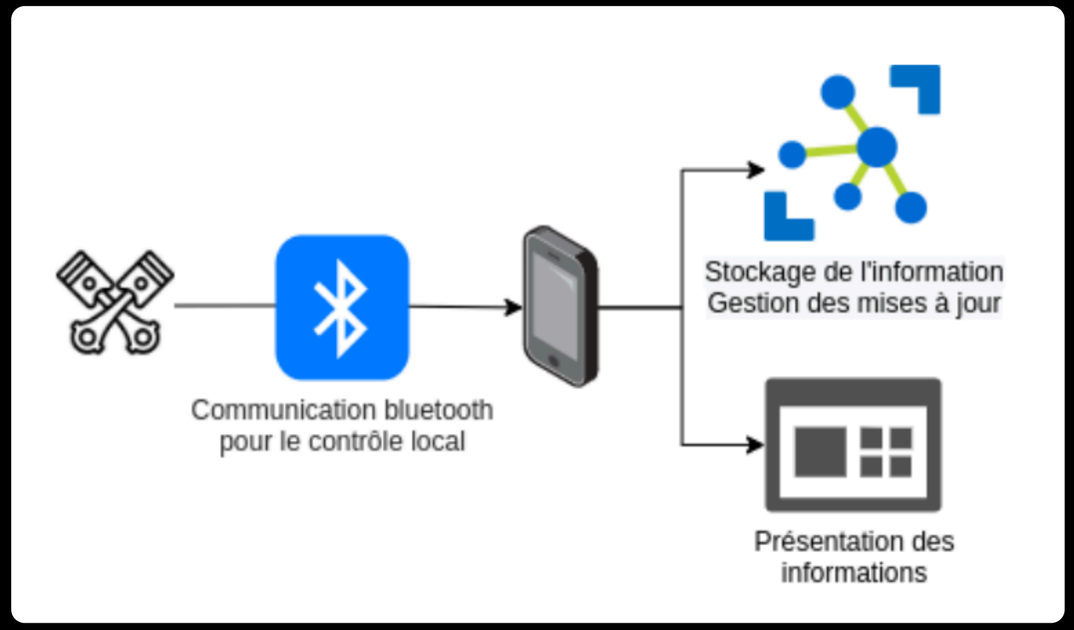
1	67	02	45	257	004	89	1 67 02 45 257 004 89
Homme	1967	Février	Département: Loiret Région: Centre-Val de Loire (anciennement Centre) Pays: France	Commune: Pressigny-les-Pins Canton: Châtillon-Coligny Arrondissement: Montargis Code Postal: 45290	Ok	Ok	Retirer espaces

En pratique

- Enrôlement et listing d’attributs
- Listing de l’ensemble des équipements
- Conversion d’URL /me > /device/UUID
- Accès aux informations des autres équipements
- Usurpation d’identité

En pratique

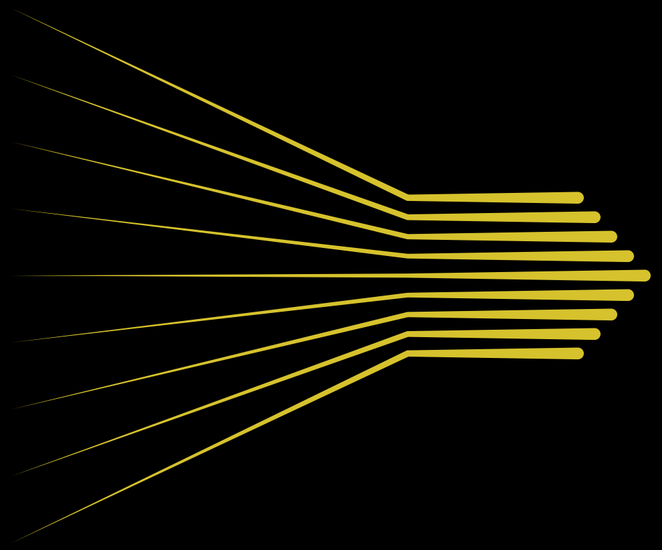
- Analyse unitaire des briques IoT
- Absence d'injection de contenu sur le Web
- Analyse de la source d'injection
- Publication MQTT à l'enrôlement
- Exploitation depuis l'affichage dashboard



Injection d'une charge XSS dans le champs propriétaire d'un équipement à l'enrôlement et exécution de cette charge lors de l'affichage des équipements sur le dashboard

En résumé

- Une donnée produite à un bout de la chaine peut n'être consommée qu'à la fin
- Un code débug VS un code production
- Un principe du moindre privilège / fonctionnalités limitant toute flexibilité
- Des identifiants unique peuvent être personnels et nécessite une protection
- Un OTP doit être désactivé après utilisation



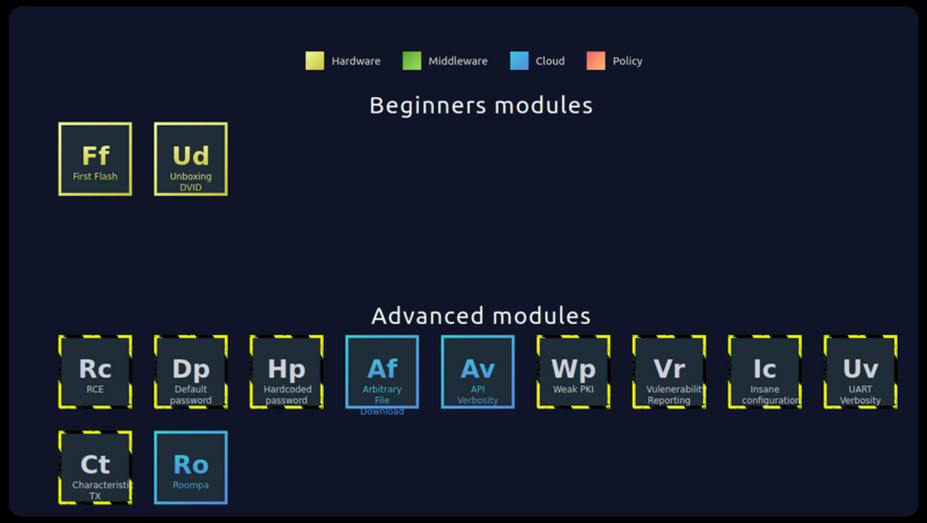
Comment anticiper une vulnérabilité et apprendre à la corriger dès les phases de conception

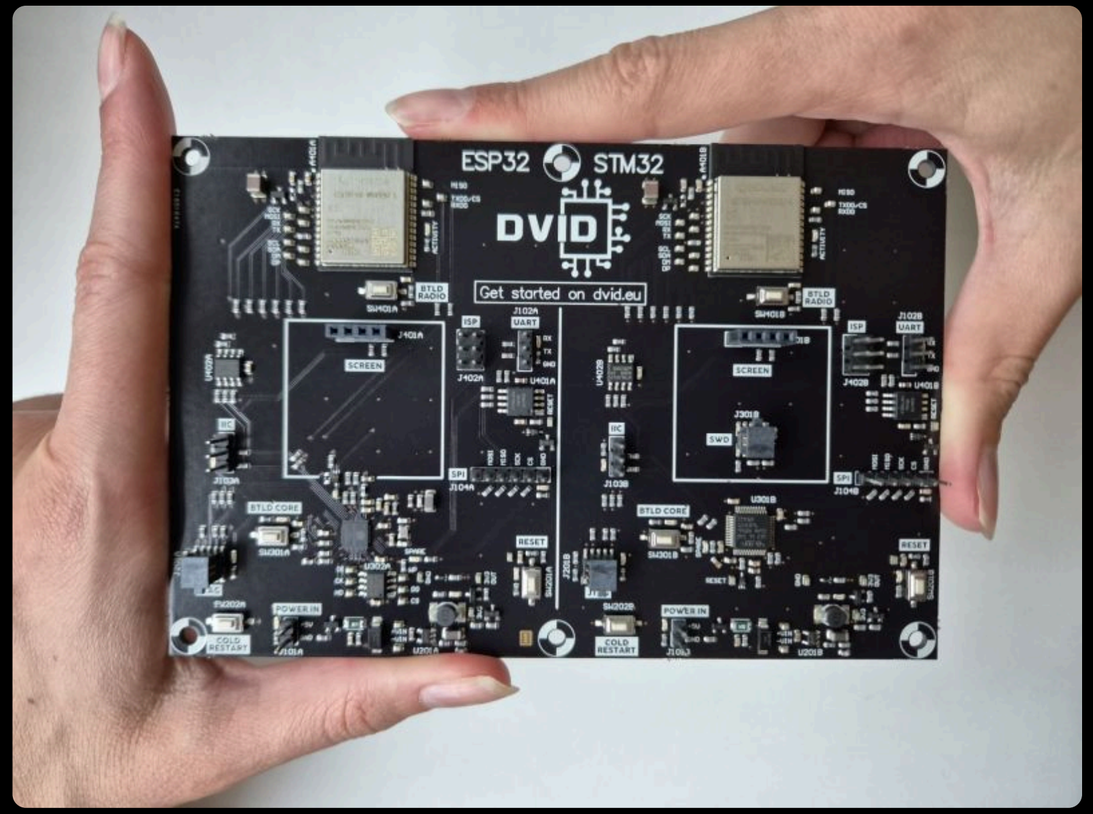
Et si on allait plus loin ?

- Expérience ludique immersive directement inspirée du monde IoT
- Outils et techniques réutilisables au quotidien en entreprise
- Une prédiction de vos problématiques suivant l'expérience collective

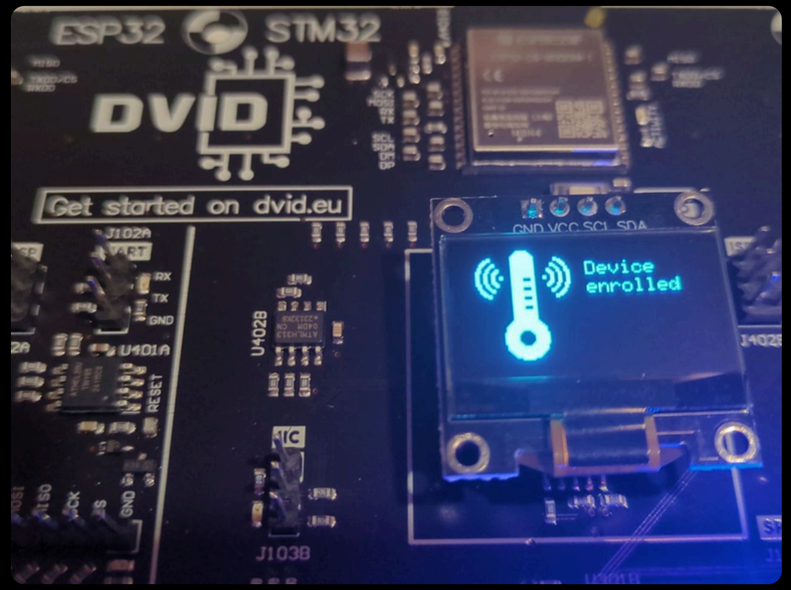
DVID EXPERIENCE

- Une carte Opensource et un SaaS online
- 400 trainings issues d’expériences terrain
- Savoir attaquer signifie savoir défendre

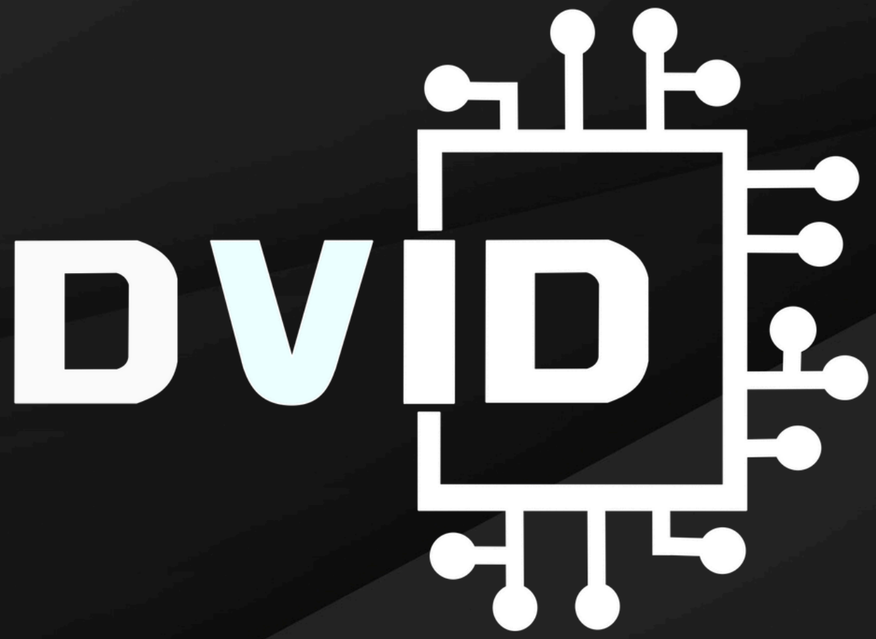




KEEP IT “OPEN”



https://github.com/dvid-security/dvidv2-opensource



READY TO ONBOARD ?

contact@dvid.eu

Keep in touch on sur dvid.eu