Le 17mai 2024

Couvent des Jacobins (Rennes)

10e édition

L’apprentissage hardware simplifié

synetis

Qui suis-je ?

MARRAZZO Samuel

Pentester sénior synetis

Formateur cyber PÔLE SUP DE LA SALLE GROUPE SAINT JEAN

Coach de l'équipe HDFR HACK-DRINK-FLAG-REPEAT

1.

POURQUOI ?

Constat études sup :

Ecoles d'ingé / Fac :

- Hardware => Electronique === Mathématiques

Autre formation :

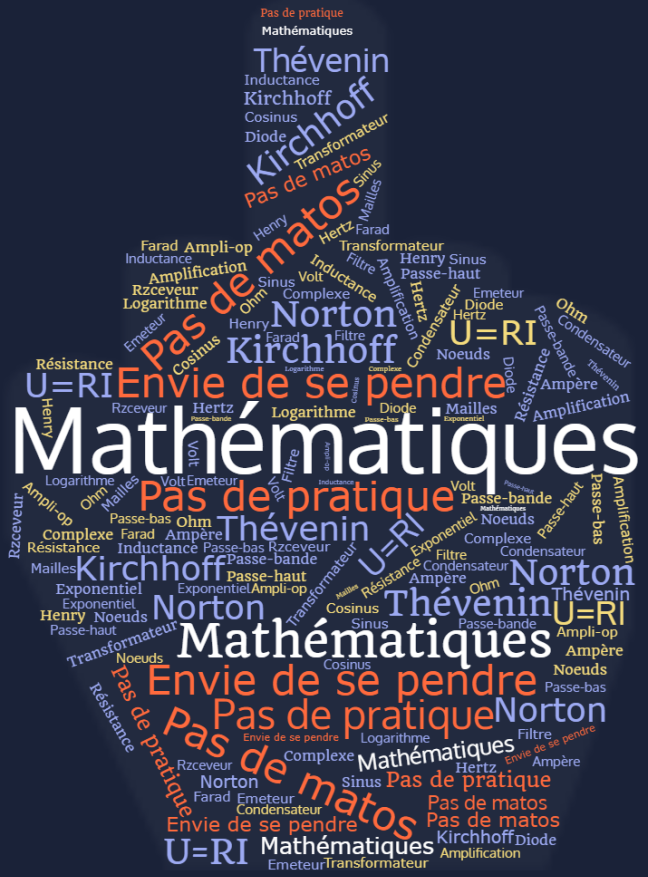
- Hardware => Pratique

Les mathématiques ne sont pas obligatoires pour faire des attaques hardwares.

Mais ça peut aider pour ne pas tout cramer.

Etudiants souhaitant faire du hardware mais n'ayant :

- Pas de connaissances mathématiques
- Pas de connaissances protocolaires (SPI, I2C, UART ….)
- Pas de connaissances documentaires (Datasheet ?)
- Pas de connaissances matériels (analyseur logique, oscillo…quoi?)

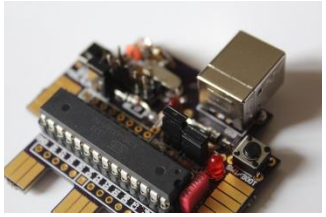


synetis

Une idée simple au départ :

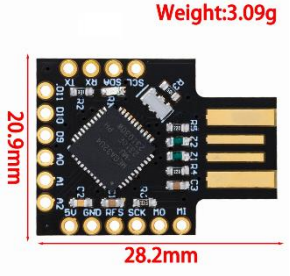
@cyberwolf_2077:

- Un mini CTF hard
- Sur un ATMega328p
- Un minimum d'outil nécessaire
- Des flags simples à trouver pour faire découvrir le Hardware



Problèmes :
- Le ATMega328p est assez vieux
- Je n'en ai qu'un seul (et j'y tiens)

Solutions :
- J'ai plein d'ATMega32U4 (Rubber Ducky du pauvre)
- Le 32U4 est l'évolution du 328p
- Caractéristiques similaires
- Plusieurs facteurs de formes
- Pas chers



synetis

@cyberwolf_2077

Rappel historique :

Apollo Guidance Computer :

- Processeur 16bits cadencé à 1Mhz
- L'équivalent de 76Ko de ROM
- L'équivalent de 4Ko de RAM

ATMega32U4 :

- Processeur 8bits cadencé à 16Mhz
- 32Ko de ROM (Flash)
- 2.5Ko de RAM
- 1Ko d'EEPROM

Revenir aux fondamentaux, avec 32 Ko de ROM et 2.5 Ko de RAM on peut faire beaucoup de chose, encore aujourd'hui.

synetis

Rappel historique :

mail.google.com

Utilisation de la mémoire :

566 Mo

2.

REALISATION

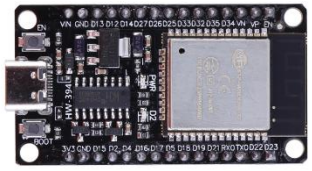
Mini CTF Hardware :

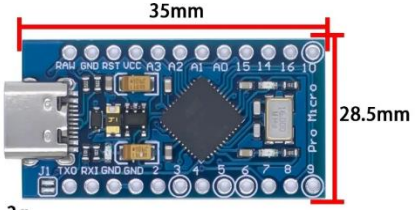
Objectifs :

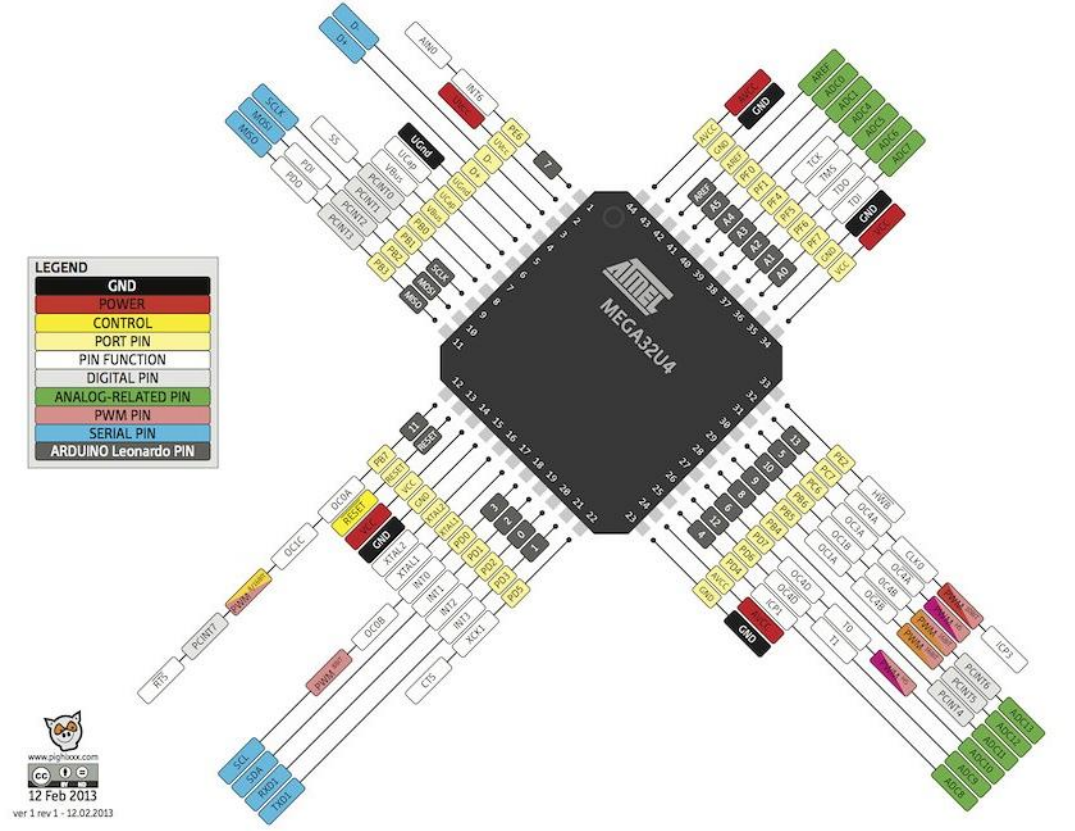
- Apprentissage de la recherche documentaire (Datasheet)
- Découverte d'un maximum de protocoles (SPI,UART,I2C, …)
- Découverte d'outils (analyseur logique, oscilloscope)
- Manipulations (breadboard, branchement des pins, glitch)
- Sélection simple des exercices
- Rappeler qu'avec quelques Ko on peut faire des trucs funs

Résultats :

- 9 Flags
- Occupation 50% ROM et 90% de RAM
- Des heures de fun (ou pas ☺)
- Multi platform -> ESP32-WROOM







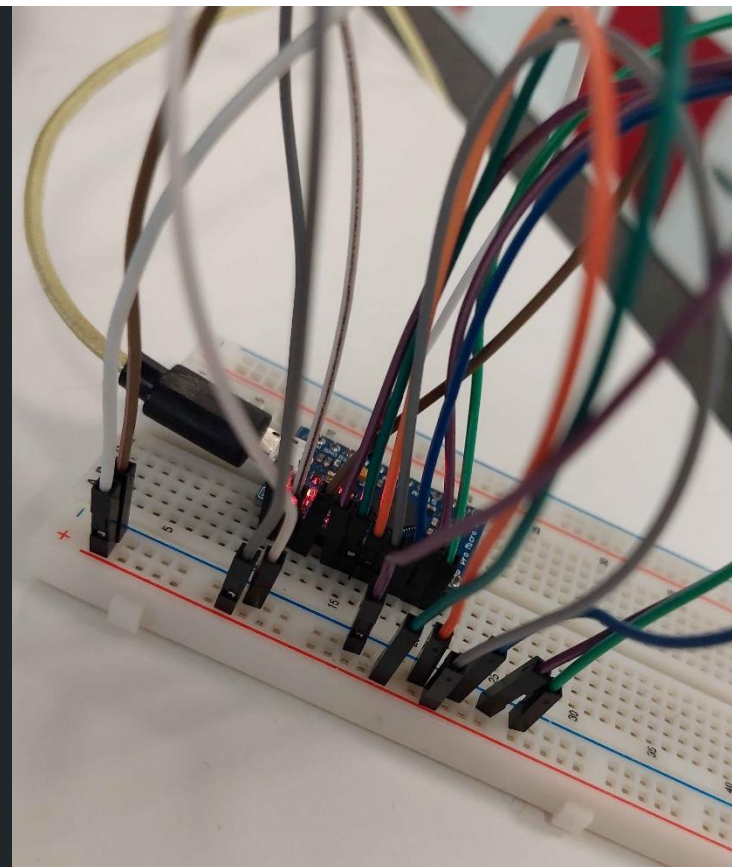
synetis

Quelques images :

```
Menu :>?

1 - Donne moi le flag !
2 - Je crois que nous avons affaire à un serial killer!
3 - Mosi et Miso sont sur un bateau ...
4 - Appel moi maître !
5 - Oui Maître !
6 - Une histoire d'écoute.
7 - Le sens de la vie.
8 - En sortie, l'union fait la force.
9 - Jouons à sha!
a - Bincat
b - Touch me !
? - Help

Menu :>
```



synetis

Samuel MARRAZZO
@EnlargeYourGeek

Suivez-nous

@BreizhCTF