

Réunion flash

Point hebdomadaire

Duzés Florian




Sommaire

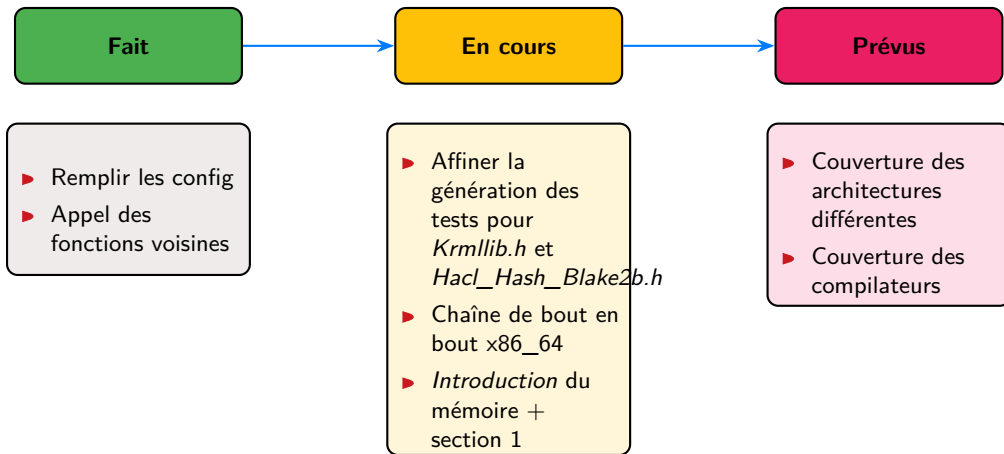
1. État des lieux
2. Axes de travaux
3. Andhrímnir
4. Érysichton
5. Conclusion

01

État des lieux

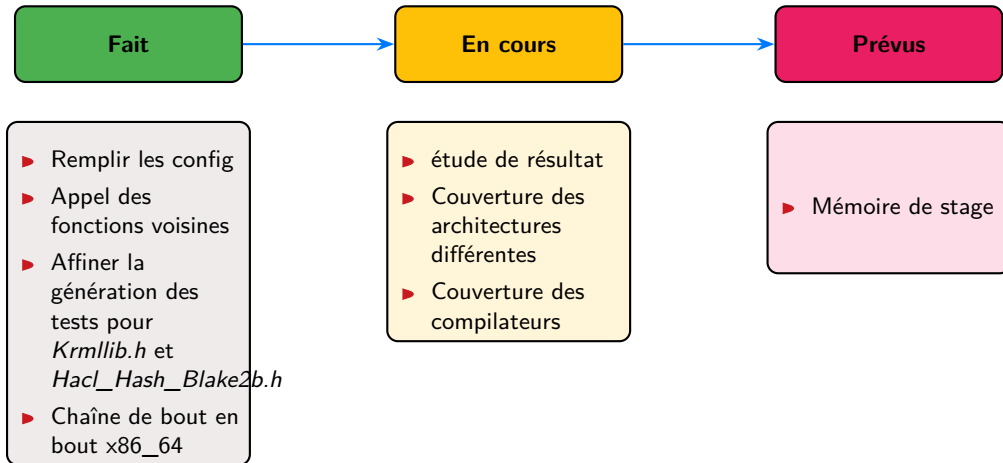


Point actuel





Réalisation



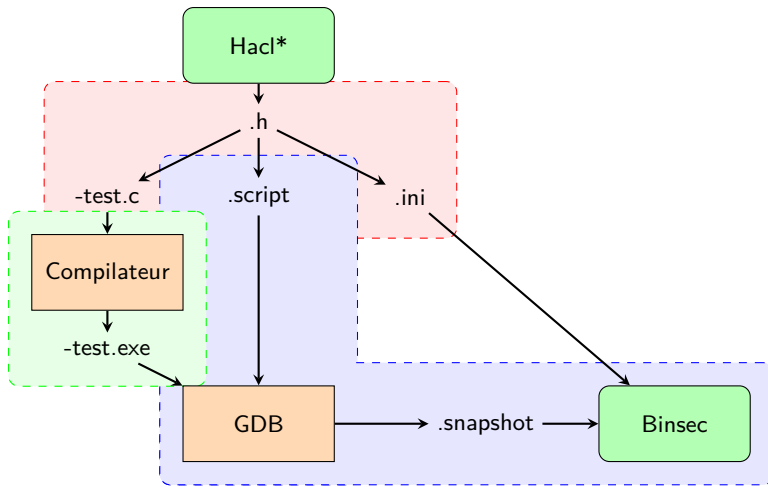
02

Axes de travaux



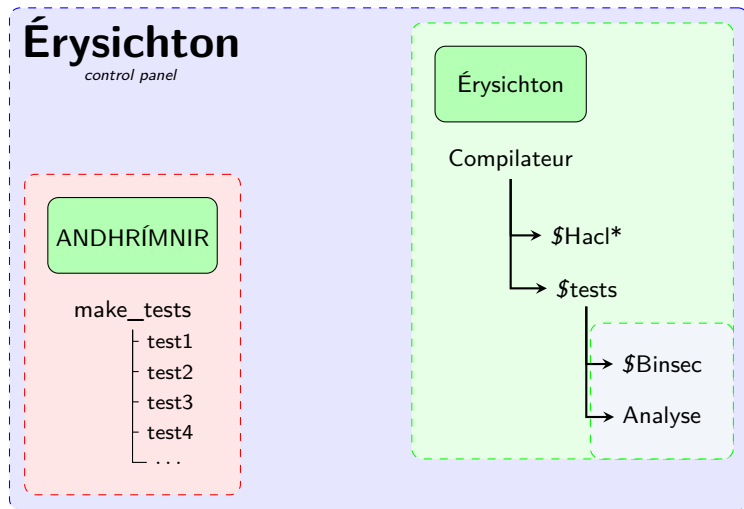


Organisation des modules



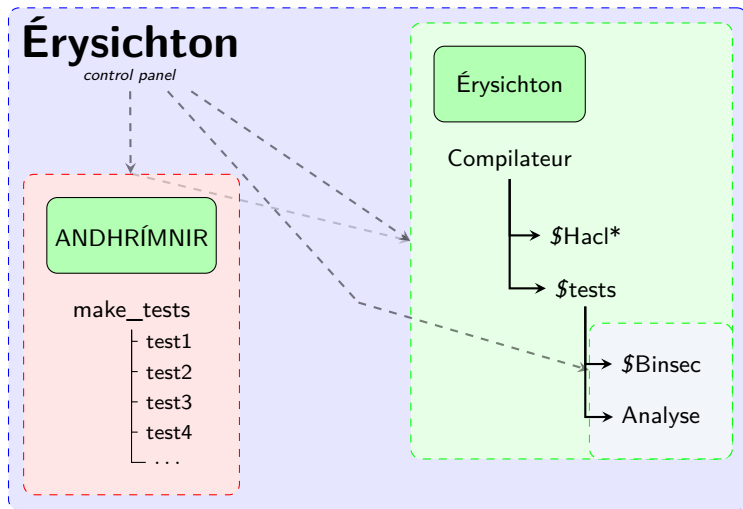


Division du travail





Division du travail



03

Andhrímnir





Cuisinier immortel

Ingrédients :

- ▶ fichier .h
- ▶ fichier de config (particulier ou blanc)

Recette :

- ▶ *\$ make tests*



Cuisinier immortel

Ingrédients :

- ▶ fichier .h
- ▶ fichier de config (particulier ou blanc)

Recette :

- ▶ *\$ make tests*

On obtient **548** fichier C prêt à être compiler.




Points d'amélioration

Limitations

- ▶ dépendances aux fichier de config
- ▶ aucune ouverture à de nouveaux fichiers

04

Érysichton





On aurait pu le nommer Sisyphe

Module x86_64 achevé

```
98% - Binsec ··· Hacl_Salsa20_salsa20_encrypt
[checkct:result] Program status is : secure (1.108)
98% - Binsec ··· Hacl_Salsa20_salsa20_key_block0
[checkct:result] Program status is : secure (0.786)
99% - Binsec ··· Hacl_SHA2_Vec128_sha224_4
[sse:error] Cut path 1 (uninterpreted "K0") @ 0x0040635c
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (0.120)
99% - Binsec ··· Hacl_SHA2_Vec128_sha256_4
[sse:error] Cut path 1 (uninterpreted "K0") @ 0x00406b1c
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (0.107)
99% - Binsec ··· Hacl_SHA2_Vec256_sha224_8
[checkct:result] Program status is : secure (3.271)
99% - Binsec ··· Hacl_SHA2_Vec256_sha256_8
[checkct:result] Program status is : secure (3.770)
99% - Binsec ··· Hacl_SHA2_Vec256_sha384_4
[checkct:result] Program status is : secure (4.242)
100% - Binsec ··· Hacl_SHA2_Vec256_sha512_4
[checkct:result] Program status is : secure (4.301)
```

Statistiques - 1

	Secure	Unknown	Insecure
Result	436	112	0
(%)	79.37	20.43	0

Table – Résultats pour une compilation sur x86_64, gcc 12.2.0

Statistiques - 2

Unknown		
<i>Total</i>		112
<i>error</i>		60
–	uninterpreted "syscall"	21
–	uninterpreted "KO"	39
<i>warning</i>	max depth	52

Table – Détails erreurs



Script Binsec

```
starting from core
halt at @[rsp, 8]
explore all
```

Code – HFStar_UInt64_eq_mask.ini

```
starting from core
secret global output, input, data, key,
    nonce, tag
halt at @[rsp, 8]
explore all
```

Code – Hacl_AEAD_Chacha20Poly1305_decrypt.ini

05

Flash info



Script Binsec

```
starting from core  
halt at @[rsp, 8]  
explore all
```

Code – *.ini

06

Conclusion





Conclusion

Objectif

~~Finir le module x86_64.~~

Un oeil plus fin

Comprendre pourquoi ces erreurs -> affiner les scripts Binsec

Augmenter

Ajouter d'autres compilateur

Merci.

