

Fraternité



Réunion flash

Point hebdomadaire

Duzés Florian

23/07/2025

Sommaire

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

01 État des lieux

Point actuel

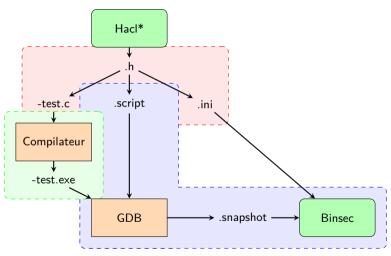
Fait Prévus En cours Affiner la Couverture des Remplir les config génération des architectures Appel des différentes tests pour fonctions voisines Krmllib.h et Couverture des Hacl Hash Blake2b.h compilateurs Chaîne de bout en bout x86 64 Introduction du mémoire + section 1

-Réalisation

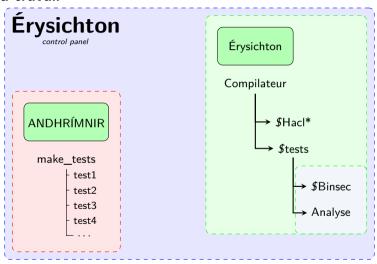
Fait En cours Prévus ▶ Remplir les config étude de résultat Couverture des Appel des Mémoire de stage fonctions voisines architectures différentes Affiner la génération des Couverture des compilateurs tests pour Krmllih h et Hacl_Hash_Blake2b.h ► Chaîne de bout en bout x86_64

02 Axes de travails

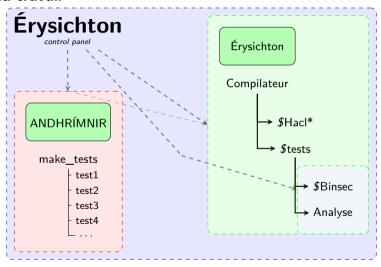
Organisation des modules



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 "KO") @ 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 "KO") @ 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)
```

23/07/2025

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		
Total		112
error		60
_	uninterpreted "syscall"	21
_	uninterpreted "KO"	39
warning	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
```

 ${\color{red}{\sf Code-Hacl_AEAD_Chacha20Poly1305_decrypt.ini}}$

05 Flash info

Script Binsec

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

Code - *.ini

06 Conclusion

Conclusion

Objectif

Finir le module ×86_64.

Un oeil plus fin

Comprendre pourquoi ces erreurs -> affiner les scripts Binsec

Augmenter

Ajouter d'autres compilateur

Merci.

23/07/2025 (nzia 21