RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inria

Réunion flash

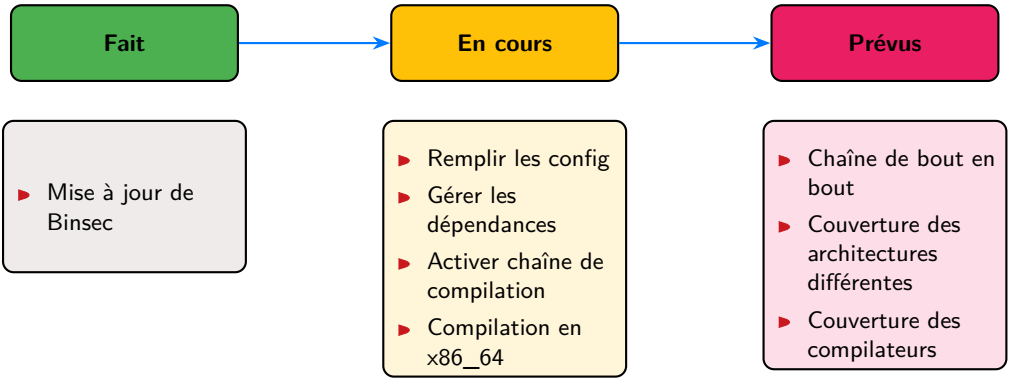
Point hebdomadaire

Duzés Florian

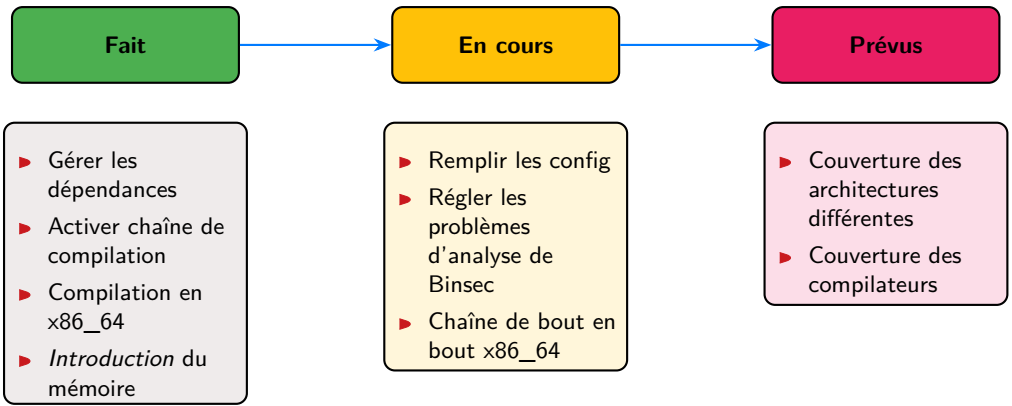
Sommaire

01
État des lieux

Point actuel



Réalisation



02
Une chaîne de bout en bout

On y est

```
florian@Core-Charpenet:~/Documents/Érysichthon_command_line$ make x86_64
Orders for x86_64 compilation ready

_____________________________________
Binsec ··· Hacl_AEAD_Chacha20Poly1305_decrypt
[checkct:result] Program status is : secure (0.929)
Binsec ··· Hacl_AEAD_Chacha20Poly1305_encrypt
[checkct:result] Program status is : secure (1.601)
Binsec ··· Hacl_AEAD_Chacha20Poly1305_Simd128_decrypt
[checkct:result] Program status is : secure (3.337)
Binsec ··· Hacl_AEAD_Chacha20Poly1305_Simd128_encrypt
[checkct:result] Program status is : secure (5.187)
Binsec ··· Hacl_AEAD_Chacha20Poly1305_Simd256_decrypt
[checkct:result] Program status is : secure (16.578)
```

Encore des problèmes

Les fichiers de config

- Remplissage à 1/3
- Gestion des exceptions
- Appel aux fonctions voisines

Encore des problèmes - 2

Analyse Binsec pas automatique

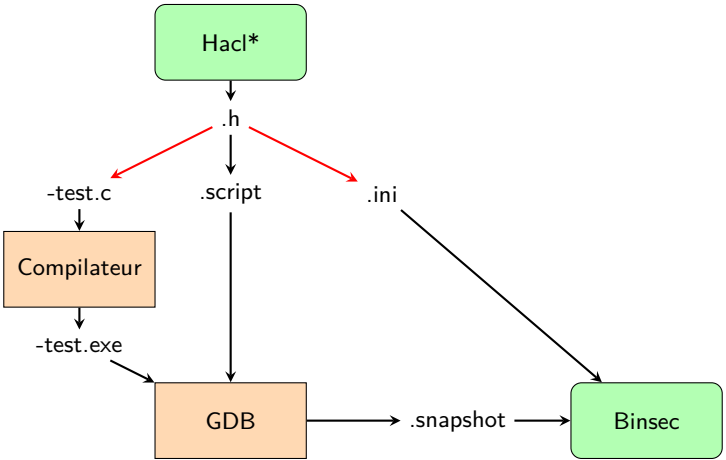
Utilisation de "core dump"

- Affectation des variables secrètes
- Proposition
  - "*" -> secret
  - liste de noms de variables

Test avec analyse directement depuis code compilé ?

03
Point avec Érysichton

Zone de difficultés



Utilisation de wrappeur

Outils

- frama-c
- clangml
- CIL

Utilisation de wrappeur

Outils

- frama-c
- clangml
- CIL

En pause pour le moment - informations déjà acquise

- *Optimisation future ?*
- Trouble avec Binsec

04
Binsec patch

Identification d'une erreur

Problème de pile

- Est-ce que le correctif est bon ?
- Compilation de binsec vers RISC-V

05
Conclusion

Conclusion

Objectif

Finir le module x86_64.

- ☐ Remplir les configurations
- ☐ Générer les tests
- ☑ ~~Compiler les tests~~
- ☑ Analyser les tests

Merci.