

# Réunion flash

Point hebdomadaire

Duzes Florian




# Sommaire

1. Bienvenue à l'INRIA
2. À l'assaut du tutoriel
3. Calendrier prévisionnel
4. Conclusion

# 01

## Bienvenue à l'INRIA





# Installation

1. Prise en main du Linux
2. Mise en place du travailleur INRIA (accès internet, profil en ligne, boîte mail, accès restauration)
3. Configuration des outils de travaux (VS Code, LaTeX)
4. Installation des librairies requises pour F\*, Hacl\*, Binsec



# Réunion de mardi

## Premier contact avec mes référents

Retour sur mon arrivée, et installation générale.

### ► Mail de référence.


- \* Installation de BINSEC (<https://github.com/binsec/binsec>) et de HACL\* (<https://github.com/hacl-star/hacl-star>). Pour HACL\*, pas besoin d'installer la toolchain F\* entière (en tout cas pour l'instant), mais assure toi de réussir à compiler le code dans `dist/gcc-compatible`, ainsi que dans `tests`
- \* Familiarisation avec BINSEC : le tutoriel est disponible ici (<https://github.com/binsec/binsec/tree/master/doc/sse>). Il peut également être utile de parcourir certains articles de recherche, particulièrement <https://binsec.github.io/assets/publications/papers/2020-sp.pdf>
- \* Application de BINSEC à HACL\* : Je te mets en pièce jointe un (court) document qui montre comment se servir de BINSEC pour analyser une des implémentations d'HACL\* (ChachaPoly avec instructions AVX). Je te conseille avant tout d'essayer de reproduire sur ta machine le processus. Une fois que ce sera fait, essaie de l'adapter à d'autres primitives cryptographiques.

## Missions claires

### ► Tutoriel Binsec à finir.

# 02

## À l'assaut du tutoriel



## Travail réalisé en deux temps

- ▶ Temps de lecture et compréhension des mécanismes
- ▶ Temps de reproduction et compilation des travaux



## Difficultés et ralentissement

- ▶ Compilation - manque de bibliothèques
- ▶ Prise en main, lecture de documentation (radare2)





## Fin du tutoriel

Tutoriel terminé jeudi<sup>1</sup>. J'ai des fichiers récapitulatif/généraux qui font office de mémo.

- ▶ protocole.md
- ▶ binsec\_ref.md

Dans la branche *git/binsec* installée en locale, j'ai modifié le tutoriel pour passer outre des difficultés rencontrés.

---

1. Je me suis appuyé sur le mail et j'ai lu les deux articles données. Constant-Time:The Pessimist Case

# 03

## Calendrier prévisionnel





## Missions enregistrées

- ▶ TUTO BINSEC -> a finir d'ici vendredi
- ▶ => 1er résultat à reproduire
  - étendre à d'autre plateforme, exploration de noyaux
  - étendre à d'autres algo
- ▶ Core dump à protocoler



# Conclusion

## Cap fixé, à l'aventure

Prochain résultats :

1. Reproduction du travail de mes aînés.
  2. Avancement dans les architectures
- 2.1 x86\_64
  - 2.2 ARM

Objectif pour le 6 mai (reste 10 jours).

*Merci.*

