RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

cea cnrs Inria

FRANCE 2030 PROGRAMME DE RECHERCHE CYBERSÉCURITÉ

Projet ARSENE - ARchitectures Sécurisées pour le Numérique Embarqué

Méthodes et outils pour la conception et le déploiement d'une implémentation RISC-V sécurisée

David Hély, Grenoble INP UGA LCIS

GRENOBLE INP UGA

anr agence nationale de la recherche

ARSENE : les contributeurs

Fédérer une communauté de recherche française en sécurité des systèmes embarqués et System-on-Chip (SOC) de manière coordonnée, structurée et durable

Un comité de suivi réunissant des futurs utilisateurs des résultats d'ARSENE : entreprises (GG et PME) et acteurs étatiques (ANSSI, DGA, AID, Comcyber)

Laboratoire	Contact Labo
ANSSI	Eliane JAULMES
CEA/LCYL	Moha AIT HMID
CEA/LFIM	Floren LEPIN
CEA/LSCO	Mickaël CARMONA
CNRS/Lab-STICC	Arnaud TISSERAND
CNRS/LHC	Lilian BOSSUET
CNRS/LIRMM	Philippe MAURINE
IMT/SAS	Jean-Max DUTERTRE
IMT/SSH	Ulrich KUHNE
Inria	Ronan LASHERMES
UGA/LCIS	Laure GONNORD
UGA/Tima	Paolo MAISTRI
UGA/Verimag	Marie-Laure POTET

IMT – Mines Saint-Etienne **: Jean Max Dutertre,** Resp. Lot 1
CNRS - Laboratoire Hubert Curien **: Lilian Bossuet,** Resp. Lot 2
Université Grenoble Alpes **: David Hély,** Coordination scientifique **Marie-Laure Potet,** Resp. Lot 3
CEA **: Romain Wacquez,** Coordination scientifique & Resp. Lot 4
Inria **: Ronan Lashermes,** Coordination INRIA

Les objectifs d'ARSENE

Proposer de nouvelles technologies et architectures de composants :

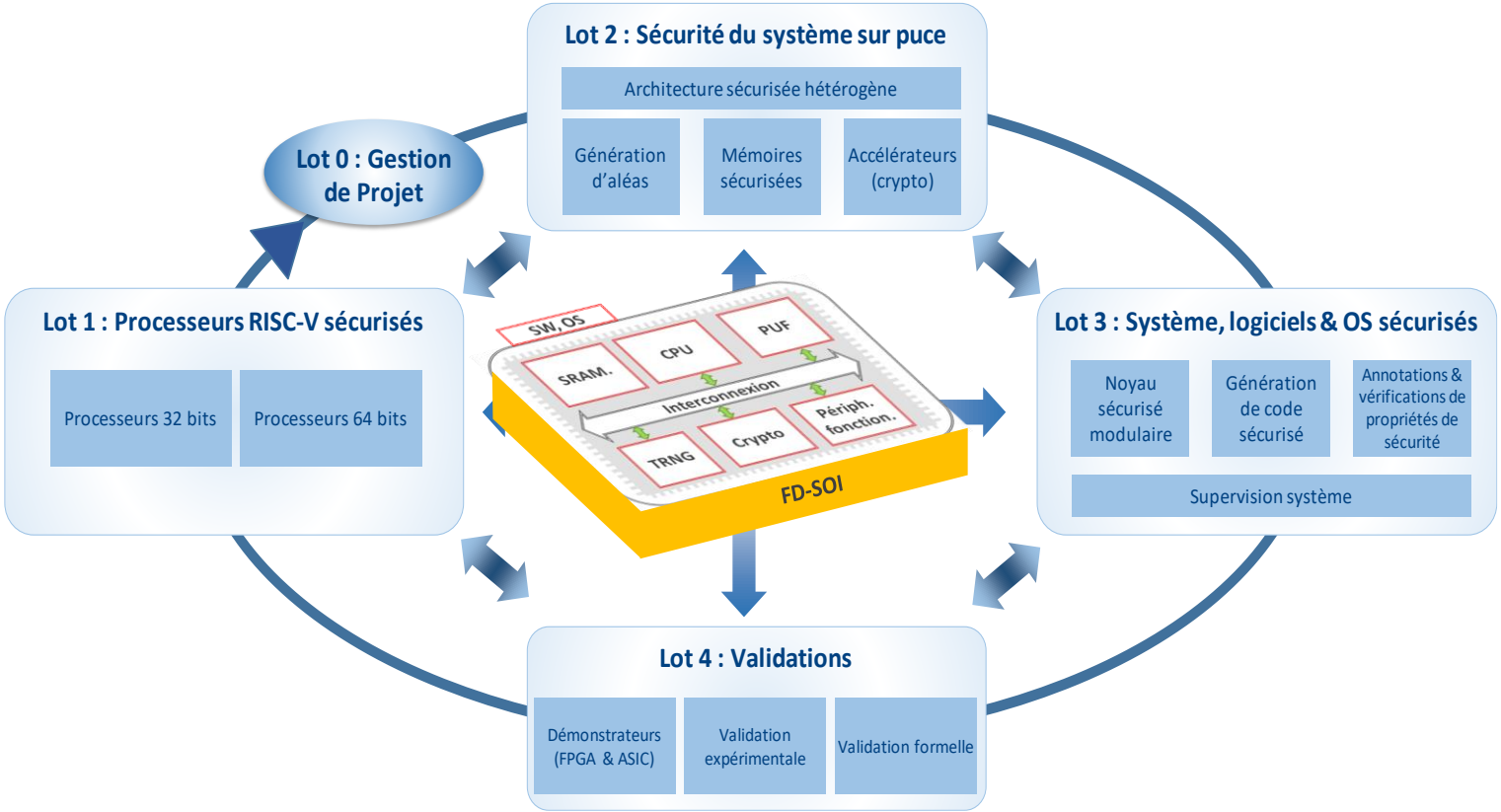
- **Résistantes à l'état de l'art** et anticipant les futures menaces matérielles
- **Adaptables à différents niveaux de sécurité** (et de certification) visés
- Intégrant **de nouvelles primitives de sécurité** adaptées aux **contraintes industrielles**
- Facilitant **une intégration efficace des couches logicielles pour une sécurité globale** (matérielle et logicielle)

Les défis d'ARSENE

Pour atteindre ces objectifs, il est nécessaire de:

- Définir et adresser **un large panel de modèles d'attaquants**
- **Modéliser à différents niveaux d'abstraction** les effets des attaques matérielles
- Permettre une **gestion agile de la sécurité tout au long du cycle de vie du produit**
- Développer de **nouvelles primitives de sécurité et contre-mesures** dont la sécurité peut être évaluée vis-à-vis de l'état de l'art
- Garantir que les choix et développements sont compatibles avec les pratiques et contraintes industrielles
- Mettre en œuvre une **approche globale de la sécurité des composants de la technologies silicium aux couches logicielles**

Les défis d'ARSENE



ARSENE et RISC-V

Pourquoi des cibles RISC-V dans Arsene?

- Souveraineté des solutions développées
- Accessibilité des architectures et des outils associés
- Contribution aux initiatives « open source »
- Continuité des travaux de recherche

RISC-V®
RISC-V: The Free and Open RISC Instruction Set Architecture

Mais aussi, le développement de RISC-V accentue certains challenges (opportunités) de sécurité

ARSENE et RISC-V

- **D'un point de vue concepteur:**
  - La caractérisation et la personnalisation de la cible sont facilitées:
    - Ajout d'instructions spécifiques pour la sécurité
    - Intégration spécifique de contre-mesures ciblées
- **D'un point de vue intégrateur**
  - L'accès aux détails de conception peut permettre une caractérisation plus précise des menaces
  - Développement de cible matérielle spécifique « démocratisée »
- **D'un point de vue développeur:**
  - Adéquation matériel-logiciel optimisée:
    - Prise en compte plus fine de l'architecture matérielle
    - Optimisation du partitionnement matériel/logiciel pour la sécurité

ARSENE et RISC-V

- **D'un point de vue concepteur:**
  - La caractérisation et la personnalisation de la cible sor
    - Ajout d'instructions spécifiques pour la sécurité
    - Intégration spécifique de contre-mesures ciblées

Validité des contre mesures?
Utilisation des contre-mesures au niveau système?

- **D'un point de vue intégrateur**
  - L'accès aux détails de conception peut permettre une
  - Développement de cible matérielle spécifique « démo

Comment exploiter aux mieux les caractérisations?
Comment garantir que l'intégration d'éléments externes ne dégrade pas la sécurité du système?

- **D'un point de vue développeur:**
  - Adéquation matériel-logiciel optimisée:
    - Prise en compte plus fine de l'architecture matéri
    - Optimisation du partitionnement matériel/logicie

Comment faciliter l'exploitation des informations bas niveau lors de la compilation?
Comment garantir que les propriétés de sécurité sont maintenues pendant la compilation?

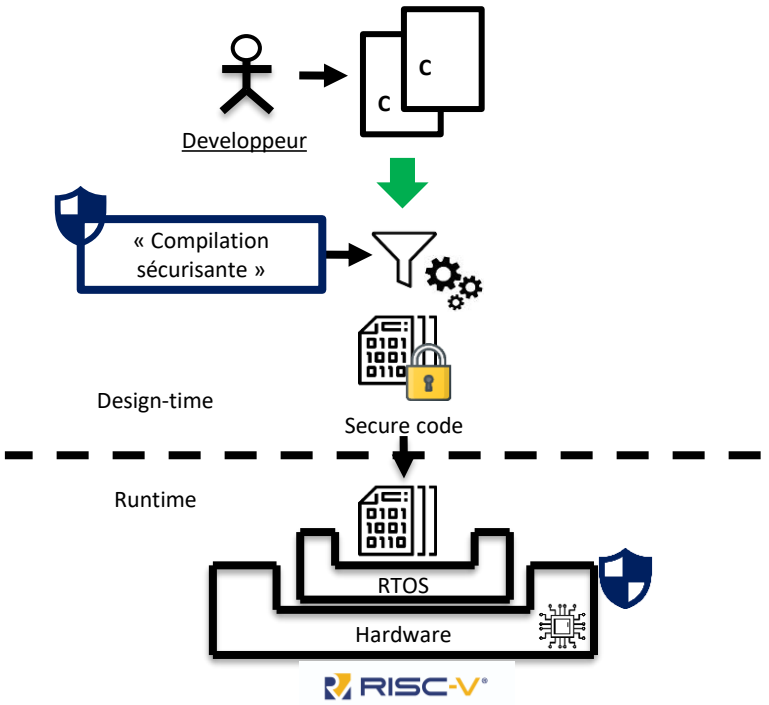
Résistance des architectures RISC-V aux attaques en fautes: une approche globale

Attaques en fautes et architectures RISC-V:

- Modélisation à **différents niveaux** des effets des attaques en fautes pour:
  - Concevoir des cibles matérielles RISC-V résistantes à ces attaques
  - Développer des compilateurs permettant de générer du code sécurisé intégrant les effets des fautes selon le degré de sécurité de la cible considérée

Défis:

- **Modélisation des effets des attaques**
- **Prise en compte de ces modèles lors de la compilation**



Résistance des architectures RISC-V aux attaques en fautes: une approche globale

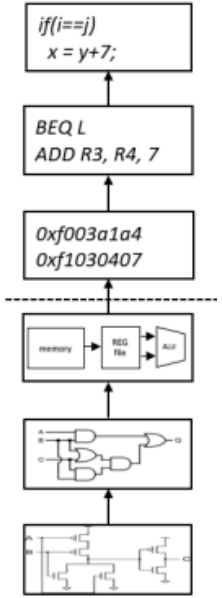
(2) Outils d'analyse multi-niveaux des effets des fautes sur le système

FDT2023: A compositional methodology to harden programs against multi-faults attacks

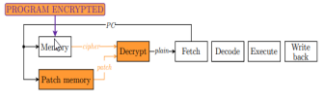
Formal Methods in CAD 2023: µArchiFI: Formal Modeling and Verification Strategies for Microarchitetural Fault Injections

CC2024:From low-level fault modeling (of a pipeline attack) to a proven hardening scheme. Compiler Construction

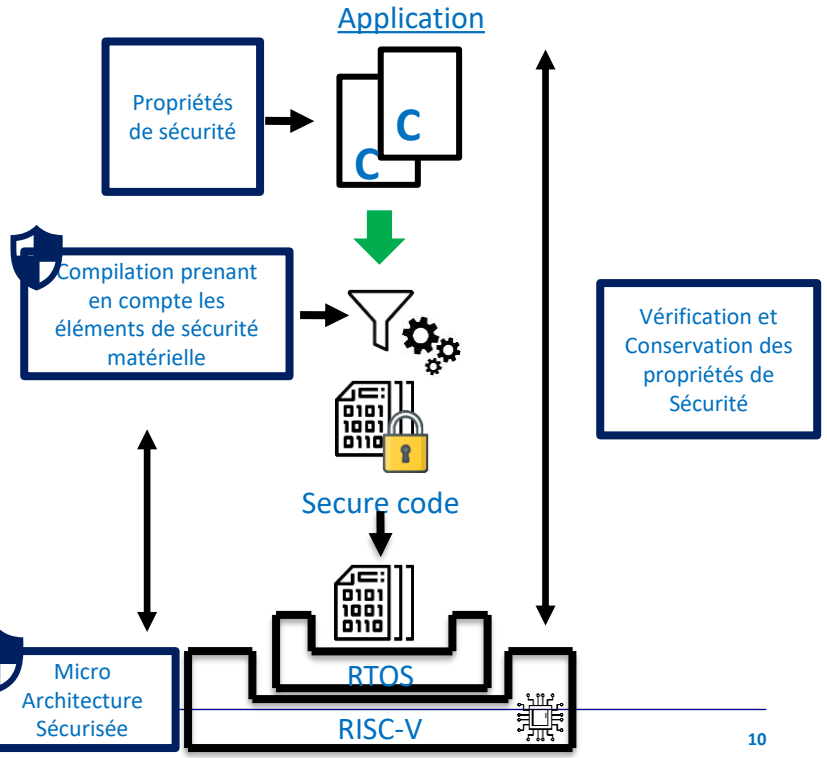
Campagne d'injections sur cible RISC-V et modélisation des fautes



Chained and Authenticated Encryption of Instructions, with Control Signal association



(4) Outils d'integration sûre des contre-mesures



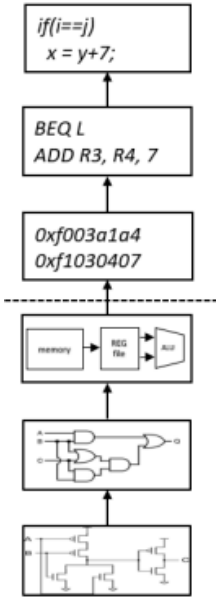
(1) Modélisation multi-niveaux des effets des attaques

(3) Conception de contre-mesures matérielles et logicielles

Résistance des architectures RISC-V aux attaques en fautes: une approche globale

(1) Modélisation des effets des fautes

- Campagnes d'injections de fautes sur cibles RISC-V:
  - Campagnes d'injections avec différents moyens (EM, power..)
  - Analyse des résultats pour:
    - Confirmer/infirmer les modèles existants
    - Mettre à jour les modèles à différents niveaux d'abstractions
  - **Caractérisation et validation d'un modèle de faute spécifique au niveau binaire exploitable plus tard dans le flot**



I. ALSHAER et al., Cross-layer inference methodology for microarchitecture-aware fault models, Microelectronics Reliability, volume 139, 2022

Résistance des architectures RISC-V aux attaques en fautes: une approche globale

(2) Caractérisation de la sensibilité aux fautes d'un système en cours de conception

- Pour une cible donnée, comment évaluer le comportement d'un logiciel soumis à des attaques en fautes?
  - **Approche co-design**:
    - **µArchiFI: Formal Modeling and Verification Strategies for Microarchitectural Fault Injections**
    - *outil open source dédié à la modélisation formelle et à la vérification des injections de fautes au niveau de la microarchitecture et de leurs effets sur les systèmes matériels/logiciels complexes*
  - **Approche logicielle:**
    - *Méthodologie pour les développeurs permettant de renforcer une application contre les attaques multi-fautes (identification des zones critiques, choix des contre mesures)*

Tollec, S., Asavoae, M., Couroussé, D., Heydemann, K., & Jan, M. (2023). µArchiFI: Formal Modeling and Verification Strategies for Microarchitetural Fault Injections. In A. Nadel & K. Y. Rozier (Eds.), *Proceedings of the 23rd Conference on Formal Methods in Computer-Aided Design – FMCAD 2023*

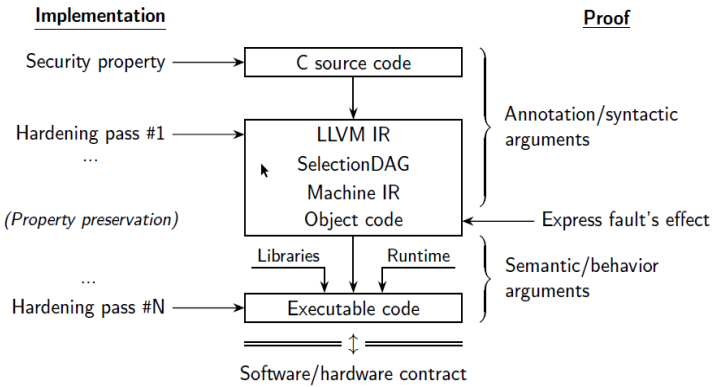
A compositional methodology to harden programs against multi-fault attacks. E. Boesflug, Laurent Mounier, Marie-Laure Potet, Abderrahmanne Bouguern. FDTC2023

Résistance des architectures RISC-V aux attaques en fautes: une approche globale

(3) Conception d'une contremesure matérielle/logicielle exploitant le modèle de faute pour garantir l'intégrité du flot d'exécution.

- ajout d'instructions spécifiques (checksum)
- Intégration de la contre-mesure dans LLVM
- Preuve formelle sur la correction de la contre-mesure

- Travaux en cours pour garantir la préservation des propriétés de sécurité à travers toutes les étapes de la compilation



Sébastien Michelland, Christophe Deleuze, Laure Gonnord. From low-level fault modeling (of a pipeline attack) to a proven hardening scheme. Compiler Construction (CC'24), Mar 2024, Edinburgh. ⟨10.1145/3640537.3641570⟩. ⟨hal-04438994⟩

Résistance des architectures RISC-V aux attaques en fautes: une approche globale

(4) Vérification des contre-mesures logicielles contre les attaques en fautes

- Est-ce que la contre mesure est:
  - **correcte**: conserve la sémantique du programme
  - **Adéquate**: protège contre un modelé de faute donnée
  - **Résistante**: n'introduit pas de nouvelles vulnérabilité?

Travaux en cours:

- Développement d'un framework de preuve intégré au **c**ompilateur prouvé CompCert/Chamois
- Elaboration de techniques permettant de garantir la préservation des contre mesures malgré les optimisations

https://gricad-gitlab.univ-grenoble-alpes.fr/certicompil/Chamois-CompCert

S. Boulmé, L. Gourdin, D. Monniaux, B. Pesin, M-L. Potet Formal Verification of Countermeasures in CompCert

Résistance des architectures RISC-V aux attaques en fautes: une approche globale

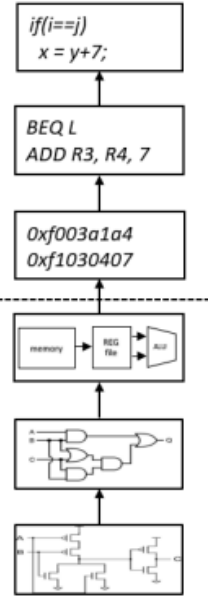
(2) Outils d'analyse multi-niveaux des effets des fautes sur le système

FDT2023: A compositional methodology to harden programs against multi-faults attacks

Formal Methods in CAD 2023: µArchiFI: Formal Modeling and Verification Strategies for Microarchitetural Fault Injections

CC2024:From low-level fault modeling (of a pipeline attack) to a proven hardening scheme. Compiler Construction

Chained and Authenticated Encryption of Instructions, with Control Signal association

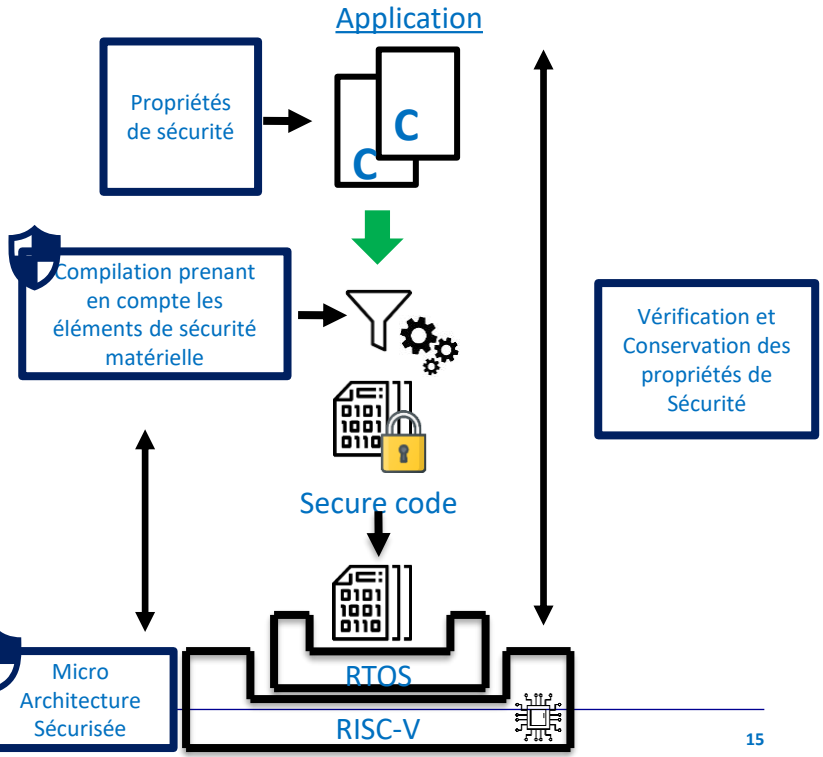


Campagne d'injections sur cible RISC-V et modélisation des fautes

(1) Modélisation multi-niveaux des effets des attaques

(3) Conception de contre-mesures matérielles et logicielles

(4) Outils d'integration sûre des contre-mesures



Au-delà des attaques en fautes…

Arsene adresse d’autres sujets importants pour une intégration sécurisée des architectures RISC-V:

- Vérification formelle de processeurs sécurisés
- Évaluation des vulnérabilités et détection d’attaques par méthode d'apprentissage
- Méthodes de sécurisation des SoC hétérogènes
- Méthodes de protection de la propriété intellectuelle dans les SoC
- Annotations de sécurité pour la compilation
- Génération de code prenant en compte les propriétés de sécurité

Conclusions

- ARSENE est un projet:
  - en phase avec les opportunités de sécurité offertes par l'architecture RISC-V
  - avec une approche globale pour une sécurité de bout en bout des systèmes sur puce

- Les méthodes et outils développés dans ARSENE sont adaptables à différentes implémentations RISC-V (et autres architectures)

- Pour en savoir plus: un workshop dédié aux travaux d'ARSENE est prévu le 7 Novembre 2024 à Valence

- Pour plus d'informations: romain.wacquez@cea.fr david.hely@grenoble-inp.fr