Camelot-OS & Sentry Kernel

CONCEPTION D'UN OS SÉCURISÉ POUR MICROCONTRÔLEURS

PLÉNIÈRE SECUREVAL - 07 AVRIL 2026

Camelot OS ?

Un OS Open-Source sécurisé

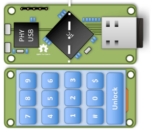
- Basé sur les résultats du projet *Wookey* (ANSSI, 2017-2021)
- Réécriture orientée usage professionnel (*Outpost-OS*, Ledger, 2021-2025)
- Devenu projet Open-Source (*Camelot-OS*, H^2Lab, 2025+)
- Support ARMv7-M et ARMv8-M, support RISC-V (RV32I) en cours de développement

Pensé pour équipements OT sécurisés

- systèmes cyber-physiques, distribués ou basse consommation
- Support temps réel initié (RMA, domaines)

Rappel des quelques projets liés à Camelot-OS

Clef USB sécurisée Wookey (ANSSI, STM32F4, 2021)

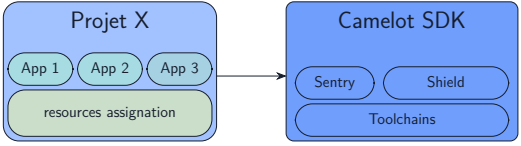


TUI sur coeur compagnon Android (i.MX8-m/Cortex-M7, Ledger, 2023)

TUI MIPI-DSI pour Secure-element (STM32U5, Ledger, 2024)

Modèle de production

- **Orienté équipes OS et équipes projets séparées**
  - Notion de *projet (besoin produit)* et de *plateforme* (besoin support)
  - SDK indépendant : outils, toolchains composants communs (noyau, runtime, etc.)
  - Projets d'intégration, prenant appui sur le SDK
- **Assure la modularité**
  - SDK personnalisable (services supports - mise à jour, gestionnaire cryptographique, etc.)
  - Projets modulaires, assignation et sécurité sous contrôle de l'intégrateur



Problématique initiale et retour d'expérience

Historique et problématique initiale

- Améliorer la **protection** du noyau contre les **fautes** (glitch, EM)
- Analyser la faisabilité de protection SW **complémentaire** du matériel
- Analyser l'impact (**sécurité**, **performance**) de contre-mesures SW

Etat des lieux : bootloader Wookey & Outpost-OS

- duplication des comparaisons : `(a == b) && !(a != b)`
  - supprimé par le compilateur, affaibli en `-O0`
  - exhaustivité dure à démontrer, résultats peu concluants
- Duplications des branches et comparaisons (gcc-14)
  - plus efficace, impact SWaP important

Défis et attendus liés à SecurEval : protection du logiciel

Protection anti-fautes à l'aide compilateur

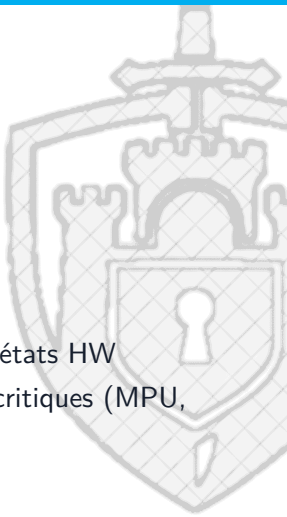
- duplication des comparaisons, redondance de calculs
- distance de Hamming, typage fort
- Injection de code défensif sur les chemins critiques
- Analyser la conformité du code généré aux attentes de protection
- Etudier l'impact SWaP des contre-mesures
- Evaluer les capacités d'un compilateur certifié (CompCert) pour cet usage

Défis et attendus liés à SecurEval : protection du logiciel

Vérification des protections par l'outillage et l'analyse

- Génération d'assertions défensives (e-acsl)
- Validation de la présence et de la conformité des protections post-compilation (e.g. Binsec)
- Evaluer la résistance des solutions sur des modèles de fautes réalistes (e.g. Lazart)
- Comparer la couverture et la complémentarité des outils

Défis et attendus liés à SecurEval : surveiller le matériel



Compenser les limitations de la protection matérielle

- Détecter les fautes ciblant les protections matérielles
  - Détection du glitch RDP (cas du bootloader Wookey)
  - Détecter la corruption des registres MPU
- Réagir à ces fautes (vérouillage, effacement, etc.)

Valider l'efficacité de l'approche mixte HW/SW

- Déterminer les faiblesses et limitations de la vérification SW des états HW
- Etudier la faisabilité (coût, performance) sur divers composants critiques (MPU, RTC, etc.)

Points clefs

- **Camelot-OS** vise un **haut niveau de sécurité** pour les systèmes embarqués à ressources limitées
- Modèle d'attaquant de Wookey
- L'usage du **formel** (noRTE, comportemental) requis
- Protection contre les fautes considérée comme **centrale**
  - pour assurer une protection adéquate contre les attaques physiques
  - doit conserver une performance et une consommation raisonnable
- Le noyau Sentry est la cible **privilégiée** à ce stade
  - d'autres services critiques hors noyau pourraient être concernés à terme (cryptographie, mise à jour sécurisée, etc.)

Références et ressources

Merci !

1. Site Camelot-OS, dépôts GitHub (H^2Lab)
2. Documentation du noyau Sentry (H^2Lab)
3. Documentation du projet Wookey (ANSSI)
4. Publication sur Wookey (ACSAC, 2019)
5. Publication Inter-CESTI, Wookey (SSTIC, 2020)
6. Publication Ledger, Outpost-OS (SSTIC, 2023)
7. Publication Ledger, Outpost-OS (SSTIC, 2024)
8. Audit de sécurité outillage Camelot-OS (H^2Lab+ANSSI+Almond, 03/2026)
9. Audit CSPN Sentry (H^2Lab+ANSSI+Almond, en cours)