Defence-related Research Action - DEFRA

ACRONYME: FORCES

Titre: FOundations for Reliable, CorrEct, and Secure robotic systems

Durée du projet: 01/12/2024 - 01/03/2029

Mots-clés: Cybersécurité, Sécurité mémoire, Transpilation de code, Robotique de défense, Évaluation des performances, Code hérité

Budget: 1.789.929 €

dont contribution IRSD: 1.663.033 €

DESCRIPTION DU PROJET

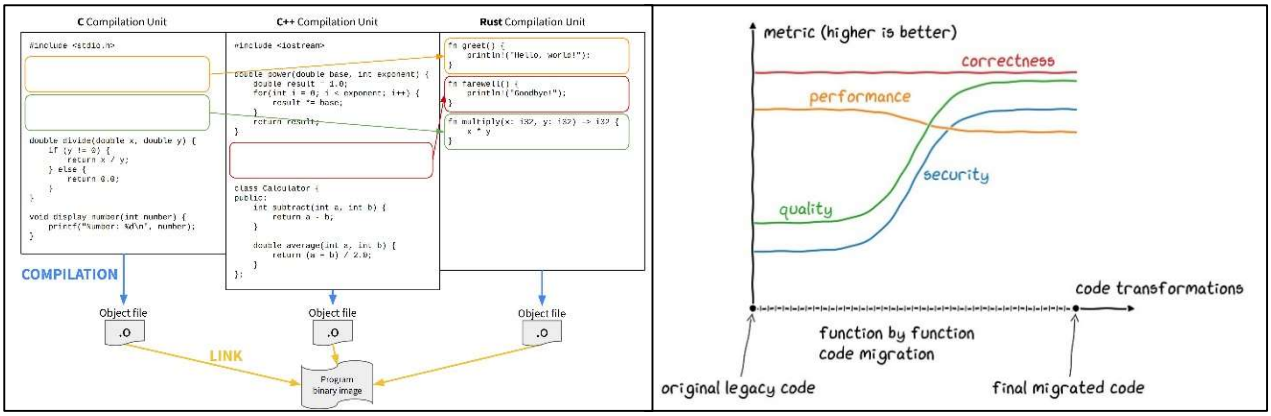
Contexte

Le projet FORCES répond à la nécessité urgente d'un logiciel plus sûr et plus sécurisé dans les systèmes de défense cyber-physiques. Les langages de programmation hérités comme C et C++ dominent les systèmes critiques de défense, mais sont intrinsèquement sujets à des vulnérabilités liées à la mémoire, posant des risques de sécurité importants. Les langages modernes comme Rust offrent une solution convaincante en garantissant la sécurité mémoire et la gestion simultanée des tâches tout en maintenant des performances élevées. Cette transition est cruciale pour les systèmes robotiques de défense, qui jouent un rôle de plus en plus important dans des missions telles que la reconnaissance et le déminage. Ces systèmes doivent s'aligner sur les plans stratégiques de défense en cybersécurité pour garantir leur sécurité et leur fiabilité face aux menaces cybernétiques en constante évolution. En se concentrant sur la migration des systèmes hérités vers Rust, FORCES répond directement à ces vulnérabilités et contribue à renforcer la résilience des infrastructures de défense critiques.

Objectifs Généraux

FORCES vise à améliorer la sécurité et l'efficacité opérationnelle des systèmes de défense grâce :

1. Au développement de **mécanismes de transpilation de code automatisés et précis** pour faciliter la migration des systèmes hérités C/C++ vers Rust. Cette méthode minimise l'effort manuel et améliore progressivement la sécurité du code.
2. A la création d'un **cadre global** incluant une analyse de sécurité, des benchmarks de performance et une validation dans des scénarios réels, garantissant que les systèmes migrés répondent aux exigences strictes de la défense.
3. A la démonstration de l'applicabilité de ces outils et méthodologies à divers cas d'utilisation de la défense, assurant leur évolutivité et leur adaptabilité aux besoins futurs.



Méthodologie
Le projet FORCES est structuré en trois phases :

1. **Recherche Fondamentale (Année 1) :** Développement de la méthodologie de transpilation et définition de métriques pour évaluer la justesse, la sécurité, la performance et la maintenabilité.
2. **Développement de Prototype (Année 2) :** Livraison d'un prototype TRL 4 de l'outil de transpilation et validation de sa fonctionnalité sur des scénarios spécifiques à la défense, tels que les systèmes robotiques et les pilotes Linux.
3. **Affinement et Expansion (Années 3-4) :** Affinement de l'outil et du cadre d'évaluation pour atteindre TRL 5, application de la méthodologie à un ensemble élargi de cas d'utilisation, et démonstration de son efficacité dans des scénarios réels de défense.

La structure du consortium garantit une approche cohérente et multidisciplinaire :

1. **VUB** apporte son expertise en langages logiciels, transformation de code et analyse des performances. Elle dirige le développement de l'outil de transpilation et effectue les benchmarks de performance dans les scénarios de défense.
2. **RMA** fournit des cas d'utilisation réels et établit des bancs d'essai pour la validation. Son expertise en robotique militaire garantit l'applicabilité des résultats à des contextes opérationnels réalistes.
3. **TBE** contribue à l'aide de son expertise en cybersécurité, définit des métriques de sécurité et évalue la sûreté du logiciel transpilé. Elle élargit également l'impact du projet en fournissant des cas d'utilisation supplémentaires liés à la défense.

Impact Potentiel sur la Défense
Le projet peut transformer les systèmes de défense en :

1. **Sécurisant la Robotique de Défense :** Amélioration de la sécurité des systèmes robotiques tels que les véhicules terrestres autonomes (UGV) et les bras robotiques, réduisant les risques liés aux vulnérabilités mémoire.
2. **Promouvant l'Innovation :** Équipement des organisations de défense avec des outils et des méthodologies avancés pour le développement de logiciels sécurisés.
3. **Modernisation Rentable :** Facilitation de la migration des systèmes hérités vers Rust, préservant la fonctionnalité tout en adressant les vulnérabilités.
4. **Élargissant l'Adoption** : Démonstration de la valeur des pratiques de programmation sécurisées dans la défense, avec des applications potentielles dans les systèmes de guidage, les infrastructures de communication et les logiciels opérationnels.

Résultats Finaux Attendus
Le projet fournira :

1. **Un outil de transpilation robuste** capable de migrer le code hérité C/C++ vers Rust, garantissant des systèmes de défense plus sûrs et plus efficaces.
2. **Un cadre d'évaluation validé** avec des métriques pour la justesse, la sécurité, la performance et la maintenabilité.
3. **Une validation dans des cas d'utilisation réels**, démontrant l'amélioration de la sécurité et des performances des systèmes robotiques.
4. **La diffusion des connaissances** via des publications dans des conférences et journaux à fort impact, ainsi que des ateliers et démonstrations pour les parties prenantes de la défense.
5. **La formation et le renforcement des capacités** des partenaires du consortium, améliorant leur expertise en cybersécurité et en pratiques de codage sécurisé.

Perspectives de Valorisation
À court terme, FORCES fournira des outils et des méthodologies pour relever les défis immédiats de la cybersécurité dans les systèmes hérités. Des ateliers et des publications sensibiliseront la communauté de défense et encourageront l'adoption.

À moyen terme, les méthodologies et outils du projet trouveront des applications élargies dans la défense et au-delà, influençant les pratiques de programmation sécurisées dans d'autres domaines critiques. L'outil pourrait également servir de base pour des projets de suivi, étendant l'approche à d'autres langages de programmation et domaines d'application.

En relevant les défis immédiats et en posant les bases des avancées futures, FORCES s'aligne sur les objectifs stratégiques de la défense et démontre la valeur de la programmation sécurisée pour les infrastructures critiques.

COORDONNÉES

Coordinateur
Paolillo
Vrije Universiteit Brussel (VUB) / Software Languages Lab
antonio.paolillo@vub.be

Partenaires
Ken Hasselmann
Ecole Royale Militaire - Koninklijke Militaire School (RMA) / RAS-lab
ken.hasselmann@mil.be

Jonathan Pisane
Thales Belgium SA
jonathan.pisane@be.thalesgroup.com

LIEN(S) DU PROJET

https://soft.vub.ac.be/forces/
https://mecatron.rma.ac.be/index.php/projects/forces/