Application BASTRI
Fiches Equipes

EVEREST (SR0178NR)

Environnements de vérification et sécurité du logiciel
EVEREST

Statut: Terminée

Responsable : Gilles Barthe

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Programmation, vérification et preuves

Période : 01/11/2004 -> 31/12/2008
Dates d'évaluation :

Etablissement(s) de rattachement : <sans>
Laboratoire(s) partenaire(s) : <sans UMR>

CRI : Centre Inria d'Université Côte d'Azur
Localisation : Centre Inria d'Université Côte d'Azur
Code structure Inria : 041014-0

Numéro RNSR : 200418404S
N° de structure Inria: SR0178NR

Présentation

L'équipe-projet EVEREST vise à promouvoir l'utilisation des méthodes formelles dans le cadre de la sécurité des systèmes. Les domaines d'application privilégiés sont les petits objets portables sécurisés, et notamment les cartes à puce, les systèmes d'exploitation, et les applications mobiles et embarquées.

Axes de recherche

Notre programme de recherche se focalise sur les trois thèmes suivants:

- plateformes sécurisées: nous concevons des plateformes sécurisées, en nous appuyant sur des méthodes vérification issues du domaine des langages de programmation, comme par exemple les systèmes de types et le code auto-certifié. Nous étudions en particulier les machines virtuelles Java et JavaCard, et les systèmes d'exploitation sécurisés. Nous modélisons les plateformes et prouvons leur correction à l'aide d'assistants à la preuve.
- vérification d'applications: nous développons JACK (Java Applet Correctness Kit), un environnement de vérification des programmes Java annotés en JML. Dans le cadre de ces travaux, nous étudions notamment un mécanisme d'insertion automatiques d'annotations JML garantissant des propriétés de sécurité génériques, et les extensions de JML. Nous développons également des mécanismes de vérification compositionnelle pour les applications Java.
- théorie: nous étudions la théorie des types, qui forme le noyau théorique des assistants de preuve que nous utilisons pour la vérification des plateformes et applications, et la logique temporelle, qui forme le noyau théorique des outils de model-checking et de vérification compositionnelle que nous utilisons pour la vérification des composants. Nous étudions également les modèles mathématiques permettant le raisonnement sur les algorithmes cryptographiques.

Relations industrielles et internationales

- ACI Sécurité GECCOO: Génération de code certifié pour les applications orientées objets: spécification, raffinement, preuve et détection d'erreurs
- ACI Sécurité Spops: Sécurité et sûreté des systèmes d'exploitation ouverts pour petits objets portables sécurisés
- Projet RNTL CASTLES: Conception d'Analyses Statiques et de Tests pour le Logiciel Embarqué Sécurisé
- Projets IST Verificard, Profundis, Types, Appsem II

Contact

- **Responsable :** Gilles Barthe
- **Tél :** 04.92.38.79.38
- **Secrétariat Tél :** 04.92.38.76.00

En savoir plus

- Site sur inria.fr
- Derniers Rapports d'Activité :

Documents sur la structure

- Intranet
- Privés

Décisions

- 4354 (01/12/2004) : création
- 5789 (11/09/2007) : prolongation
- 6519 (11/02/2009) : fermeture

Localisation

- **Adresse postale :** Centre Inria d'Université Côte d'Azur 2004 Route des Lucioles - BP 93 06902 Sophia Antipolis cedex France
- **Coordonnées GPS :** 43.616, 7.068