Application BASTRI
Fiches Equipes

CASSIS (SR0055XR)

Combinaison d'approches pour la sécurité des systèmes infinis
CASSIS PESTO (SR0729KR)

Statut: Terminée

Responsable : Michael Rusinowitch

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 : Sécurité et confidentialité

Période : 01/04/2003 -> 31/12/2015
Dates d'évaluation : 22/03/2011 , 17/03/2015

Etablissement(s) de rattachement : CNRS, U. DE FR.-COMTÉ, U. DE LORRAINE
Laboratoire(s) partenaire(s) : LORIA, FEMTO-ST (6174)

CRI : Centre Inria de l'Université de Lorraine
Localisation : Bâtiment Ada Lovelace - Centre Inria de l'Université de Lorraine
Code structure Inria : 051007-0
CRI : Centre Inria de l'Université de Lorraine
Localisation : Besançon
Code structure Inria : 051007-0

Numéro RNSR : 200318302K
N° de structure Inria: SR0055XR

Présentation

L'objectif de l'équipe-projet est la conception et la réalisation d'outils pour vérifier la sûreté des systèmes à nombre infini d'états. Notre analyse des systèmes se fonde sur une représentation symbolique des ensembles d'états comme langages formels ou formules logiques. La sûreté est obtenue par la preuve automatique, l'exploration symbolique de modèles, ou la génération de tests. Ces méthodes de validation sont complémentaires mais s'appuient, dans notre équipe-projet, sur l'étude de problèmes d'accessibilité et leur réduction à des résolutions de contraintes.
Une originalité de l'équipe-projet réside dans sa focalisation sur les systèmes infinis, paramétrés ou de grande taille, sur lesquels chaque technique prise séparément montre ses limites. Comme exemples de tels systèmes nous pouvons citer les protocoles opérant sur des topologies de taille arbitraire (réseaux en anneaux), les systèmes manipulant des structures de données de taille quelconque (ensembles), ou dont le contrôle est infini (automates communicants par tampon non borné).
Les applications visées ou en cours sont les logiciels embarqués par exemple sur cartes à puce, les protocoles de sécurité et les systèmes répartis.

Axes de recherche

L'élaboration de méthodes et d'outils de vérification de logiciels critiques est notre objectif. Pour le réaliser, nous développons de manière conjointe des techniques de preuve pour la sécurité de logiciels, de résolution de contraintes ensemblistes pour la génération de tests et d'analyse d'atteignabilité pour la vérification de systèmes infinis.

- *Preuve automatique :*
  Le but est de prouver la validité d'assertions issues de l'analyse des programmes. Nous développons des techniques et des systèmes de déduction automatique fondés sur la réécriture et la résolution de contraintes. La vérification de structures de données récursives fait fréquemment appel à des raisonnements par récurrence, ou à la manipulation d'équations, et exploite des propriétés d'opérateurs comme l'associativité ou la commutativité.
- *Synthèse et résolution de contraintes ensemblistes :*
  L'objectif de cet axe porte sur l'évaluation de spécifications formelles logico-ensemblistes. Les travaux actuels concernent le développement d'un système de résolution de contraintes ensemblistes autour du

Contact

- **Responsable :** Michael Rusinowitch
- **Tél :** 03.83.59.30.20
- **Secrétariat Tél :** 03.83.59.30.54

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 3814 (03/04/2003) : création
- 5789 (11/09/2007) : prolongation
- 7611 (03/01/2011) : prolongation
- 8339 (19/01/2012) : prolongation

Localisation

- **Adresse postale :** Centre Inria de l'Université de Lorraine, Bâtiment Ada Lovelace, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy France
- **Coordonnées GPS :** 48.666, 6.157

noyau CLPS.
- *Analyse d'atteignabilité dans les systèmes infinis :*
  L'objectif principal de cet axe est de savoir déterminer si des états non désirables peuvent être ou non atteints par un système de grande taille ou infini. Cette problématique de l'atteignabilité d'états est évidemment centrale pour garantir la sécurité des systèmes critiques.

Les domaines d'application actuels de l'équipe sont :

- *Vérification de protocoles de sécurité :*
  Les protocoles de sécurité comme SET, TLS, Kerberos sont conçus pour établir la confiance lors des transactions électroniques. Ils reposent sur des primitives cryptographiques visant à assurer l'intégrité des données, l'authentification ou l'anonymat des participants, la confidentialité des transactions, etc. L'expérience a montré que la conception de ces protocoles est souvent erronée, même en admettant que la cryptographie est parfaite, c'est-à-dire qu'un message codé ne peut être décrypté sans la clé. Un adversaire peut intercepter, analyser et modifier les messages échangés avec peu de moyens de calculs et causer par exemple des dégats économiques importants. L'analyse des protocoles cryptographiques est complexe car l'ensemble de configurations à envisager est immense voire infini : il faut prendre en compte un nombre quelconque de sessions, une taille quelconque des messages, l'entrelacement des sessions, les propriétés algébriques du cryptage ou des structures de données. Notre approche consiste à automatiser au maximum l'analyse des protocoles, à partir de leurs spécifications. Le système CASRUL que nous développons compile les spécifications avant de les soumettre à des procédures de décisions.
- *Génération de séquences de tests à partir d'un modèle formel :*
  Une application de notre système de résolution de contraintes ensemblistes est le génération de séquences de tests. Elle repose sur l'extraction des valeurs limites pour les variables d'états de la spécification pour ensuite calculer les séquences d'opérations permettant de mettre le système dans ces états aux limites. Dans les deux phases, la technique met en oeuvre le solveur de contraintes ensemblistes.

Logiciels

- haRVey
- Casrul
- daTac
- BZ-Testing-Tools
- Spike

Relations industrielles et internationales

Partenariats industriels :

- Depuis 1997, une collaboration de fond est engagée avec la société SchlumbergerSema, division Test et Transaction, pour la formalisation de spécifications techniques de besoins et la génération de séquences de tests à partir du modèle formel.
- L'ANVAR, dans le cadre des procédures d'aide à l'innovation, soutient le développement de l'environnement BZ-Testing-Tool, sa consolidation et son durcissement pour diffusion en logiciel libre de droits pour un usage non commercial, sur 2001-2003.

Relations internationales :

- Nous participons au programme européen : Information Society Technologies (IST), dans le cadre du FET Open Project AVISPA (IST-2001-39252) pour 2002-2005 avec l'ETH Zürich, l'Università di Genova et Siemens Münich. L'objectif de cette équipe-projet est de formaliser et de valider un corpus représentatif de protocoles internet sélectionnés dans les drafts de l'IETF, et de construire un analyseur performant pour des protocoles décrits par des spécifications complexes.
- Nous collaborons avec Ralf Kuesters de l'Université de Kiel, dans le cadre du programme d'actions intégrées franco-allemand, PAI Procope.
- Nous collaborons avec SUP'COM (École Supérieure des Communications de Tunis), dans le cadre d'un projet STIC avec A. Bouhoula, sur le thème : vérification formelle pour les logiciels de télécommunication.
- Sur le volet de la génération de tests, un partenariat est en cours avec l'Université de Waikato, Hamilton, en Nouvelle Zélande, professeur Marc Utting (en semestre invité au LIFC de juillet 2001 à janvier 2002), avec un soutien du programme de coopération scientifique franco-néo-zélandais.
- Nous faisons partie du réseau de recherche franco-québécois CPCFQ sur la sécurisation des protocoles cryptographiques.

Nous participons à une Action Concertée Incitative Cryptologie du Ministère de la Recherche sur la vérification de protocoles de sécurité (VERNAM, 2001-2003) avec l'université de Provence (R. Amadio et D. Lugiez) et l'ENS Cachan (H. Comon et J. Goubault-Larrecq).
Nous collaborons également avec les universités de Dublin, Vérone, EPFL Lausanne, Oran, OGE Oregon, SUNY Albany, Stanford, Grenoble, Orléans.