Application BASTRI
Fiches Equipes

COMETE (SR0134KR)

Vie privée, équité et robustesse dans la gestion de l'information
COMETE

Statut: Décision signée

Responsable : Catuscia Palamidessi

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : A2.1.1. Sémantique des langages de programmation , A2.1.5. Programmation par contraintes , A2.1.6. Programmation concurrente , A2.1.9. Langages synchrones , A2.4.1. Analyse , A3.4. Apprentissage et statistiques , A3.5. Réseaux sociaux , A4.1. Analyse de la menace , A4.5. Méthodes formelles pour la sécurité , A4.8. Technologies pour la protection de la vie privée , A8.6. Théorie de l'information , A8.11. Théorie des jeux , A9.1. Connaissances , A9.2. Apprentissage , A9.7. Algorithmique de l'intelligence artificielle , A9.9. IA distribuée, multi-agents

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : B6.1. Industrie du logiciel , B6.6. Systèmes embarqués , B9.5.1. Informatique , B9.6.10. Humanités numériques , B9.9. Ethique , B9.10. Confidentialité, vie privée

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Sécurité et confidentialité

Période : 01/01/2008 -> 01/12/2025
Dates d'évaluation : 22/03/2011 , 17/03/2015 , 21/03/2019 ,

Etablissement(s) de rattachement : CNRS, IP-PARIS
Laboratoire(s) partenaire(s) : LIX (UMR7161)

CRI : Centre Inria de Saclay
Localisation : Centre de recherche Inria de Saclay
Code structure Inria : 111012-1

Numéro RNSR : 200818369L
N° de structure Inria: SR0134KR

Présentation

L'équipe-projet COMETE étudie les concepts émergeant de l'ère moderne de l'informatique. La sécurité et la protection de la vie privée sont parmi les préoccupations fondamentales qui se posent dans ce contexte: l'interaction fréquente entre les utilisateurs et les appareils électroniques, et la connexion continue entre ces appareils et l'Internet, offrent aux agents malveillants la possibilité de recueillir et stocker une énorme quantité d'informations sans même que les utilisateurs soient conscients. En plus des problèmes de sécurité, les problèmes de la correction, de robustesse et de fiabilité sont rendus plus difficiles par la complexité des systèmes modernes, car ils sont très concurrents et distribués. En dépit d'être basés sur des technologies d'ingénierie impressionnantes, ils sont toujours sujet à un comportement défectueux en raison d'erreurs dans la conception du logiciel.

Pour faire face à ces défis, nous étudions des cadres formels pour la spécification de ces systèmes, des théories permettant de définir les propriétés souhaitées de correction et de sécurité, ainsi que des méthodes et des techniques pour prouver qu'un système satisfait ces propriétés.

Axes de recherche

- Sécurité et protection de la vie privée: Nous sommes intéressés par le problème de la fuite d'informations secrètes à travers des observables publics. Idéalement, on voudrait que les systèmes soient complètement sécurisés, mais dans la pratique cet objectif est souvent impossible à atteindre. Par conséquent, nous avons besoin de raisonner sur la quantité d'informations divulguées, le gain de l'adversaire de cette fuite et le compromis entre la vie privée et l'utilité fournie à l'utilisateur.
- Vie privée et géolocalisation: nous étudions le problème de l'accès aux systèmes basés sur la localisation tout en protégeant l'emplacement de l'utilisateur, en ajoutant du bruit contrôlé à la position rapportée.
- Expressivité des formalismes concomitants: Nous étudions les modèles et les langages computationnels pour les systèmes distribués,

Contact

- **Responsable :** Catuscia Palamidessi
- **Tél :** 01.74.85.42.49
- **Secrétariat Tél :** 01.74.85.42.89

En savoir plus

- Site sur inria.fr
- Derniers Rapports d'Activité : 2015 , 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023

Documents sur la structure

- Intranet
- Privés

Décisions

- 6135 (04/04/2008) : création
- 8339 (19/01/2012) : prolongation
- 11318 (14/12/2015) : prolongation
- 14060 (30/12/2019) : prolongation
- 14351 (25/06/2020) : prolongation
- 14489 (21/10/2020) : prolongation
- 14793 (04/05/2021) : prolongation
- 15191 (01/12/2021) : création

Localisation

- **Adresse postale :** Centre de recherche Inria de Saclay Campus de l'École Polytechnique - Bâtiment Alan Turing 1 rue Honoré d'Estienne d'Orves 91120 Palaiseau France
- **Coordonnées GPS :** 48.714, 2.206

probabilistes et mobiles, en accordant une attention particulière aux questions d'expressivité. Nous cherchons à développer des critères pour évaluer le pouvoir expressif d'un modèle ou d'un formalisme dans un cadre distribué, comparer des modèles et des formalismes existants, et en définir des nouveaux selon le niveau d'expressivité souhaité.
- Programmation concurrente par contraintes: un modèle bien établi pour la spécification de systèmes concurrents où les agents ajoutent de l'information ou interrogent si certains faits peuvent être déduits. Notre recherche se concentre sur l'étude de la sémantique de bisimulation pour ccp, ainsi que sur l'extension de ccp avec des constructions pour capturer des systèmes émergeants tels que ceux dans les réseaux sociaux et le cloud computing.
- Verification: on s'intéresse à développer des techniques de verification pour des systèmes concurrents, en mettant l'accent sur la preuve qu'un système satisfait les propriétés de sécurité ou de vie privée souhaitées.

Logiciels

- Location Guard: une extension de navigateur qui permet de protéger votre position lors de l'utilisation de sites web avec géolocalisation intégrée, en y ajoutant du bruit contrôlé.
- libqif: L'objectif de libqif est de fournir une boîte à outils C++ efficace mettant en œuvre une variété de techniques et d'algorithmes dans les domaines de "quantitative information flow" et de "differential privacy".
- D-SPACES: Une implémentation de systèmes de contraintes avec des opérateurs d'espace et d'extrusion.

Relations industrielles et internationales

- Collaboration avec Renault sur la protection de la vie privée des voitures "connectées"
- Une collaboration régulière avec plusieurs partenaires internationaux, parmi lesquels: Geoffrey Smith (Florida International University, United States), Carroll Morgan (NICTA, Australia), Annabelle McIver (Macquarie University, Australia), Moreno Falaschi (University of Siena, Italy), Mario Ferreira Alvim Junior (Federal University of Minas Gerais, Brazil), Camilo Rueda (Universidad Javeriana Cali, Colombia)
- CRYPTECS: projet in the contexte de la ANR-BMBF French-German Joint Call on Cybersecurity. Le but est de créer une "open source cloud platform promoting the adoption of privacy-preserving computing". Les partenaires sont: Orange (France), The Bosch Group (Germany), Inria COMETE (France), the University of Stuttgart (Germany), Zama (SME spin-off of CryptoExperts, France), et Edgeless Systems (SME, Germany)
- LOGIS: Logical and Formal Methods for Information Security, Equipe Associée Inria. Partenaires internationaux: Keio University (Japan), AIST (Japan), JAIST (Japan), University of Tokyo (Japan)
- REPAS: Reliable and Privacy-Aware Software Systems via Bisimulation Metrics, projet ANR. Partenaires internationaux: University of Bologna (Italy)
- FACTS: projet ECOS NORD "Foundational Approach to Cognition in Today's Society". Les partenaires sont: Inria COMETE (France), LIP6, Sorbonne University (France), et Universidad Javeriana de Cali (Colombia).