Application BASTRI

Fiches Equipes

SECSI (SR0565JR)

Sécurité des systèmes d'information
SECSI (SR0142GR) SECSI

Statut: Terminée

Responsable : Jean Goubault-larrecq

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 : 01/01/2013 -> 31/12/2013
Dates d'évaluation : 22/03/2011

Etablissement(s) de rattachement : CNRS, ENS CACHAN
Laboratoire(s) partenaire(s) : LSV (UMR8643)

CRI : Centre Inria de Saclay
Localisation : ENS Cachan - Laboratoire Spécification et Vérification (LSV)
Code structure Inria : 111030-1

Numéro RNSR : 200218376V
N° de structure Inria: SR0565JR

Présentation

L'équipe-projet SECSI est une équipe de recherche sur la sécurité des systèmes d'information. Elle est organisée autour de trois axes, et de leurs relations mutuelles:

- Vérification de protocoles cryptographiques;
- Détection d'intrusions;
- Analyse statique de programmes, dans le but de détecter des trous de sécurité et des vulnérabilités au niveau protocolaire.

Axes de recherche

- Sécurité des protocoles cryptographiques: confidentialité, authentication, fraîcheur, quant-à-soi, anonymat.
- Automates d'arbres, contraintes ensemblistes, sous-classes décidables de la logique du premier ordre et codages/approximations de processus cryptographiques parallèles.
- Détection d'intrusions, vérification de modèles efficace en ligne avec application à la détection et au reporting d'événements composés.
- Analyse statique, en particulier à base de domaines abstraits d'automates d'arbres pour l'analyse de formes et de propriétés de sécurité.

Relations industrielles et internationales

Projets nationaux

- Le projet RNTL EVA (explication et vérification automatique de protocoles cryptographiques).
- Le projet DICO (détection d'intrusions coopérative).

Actions concertées incitatives

- L'ACI Crypto VERNAM (sous-classes de protocoles cryptographiques).
- L'ACI Crypto PSI-Robuste (sécurité des programmes à base de cryptographie).
- L'ACI "Jeunes Chercheurs" Sécurité informatique, protocoles cryptographiques et détection d'intrusions (relations entre vérification de protocoles cryptographiques et détection d'intrusions).

Contact

- **Responsable :** Jean Goubault-larrecq
- **Tél :** 01.47.40.75.68
- **Secrétariat Tél :** 01.47.40.75.17

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 9165 (28/01/2013) : création
- 9166 (28/01/2013) : nomination responsable

Localisation

- **Adresse postale :** ENS Cachan - Laboratoire Spécification et Vérification (LSV) 61 Avenue du Président Wilson, 94230 Cachan Cedex France
- **Coordonnées GPS :** 48.789083, 2.326444