Application BASTRI

Fiches Equipes

SUSHI (SR0951JR)

Sécurité à l'interface logiciel/matériel
CIDRE (SR0450UR) SUSHI

Statut: Décision signée

Responsable : Guillaume Hiet

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : A1.1.2. Accélérateurs matériels (GPGPU, FPGA, DSP, etc.) , A1.1.8. Sécurité des architectures , A1.1.10. Architectures reconfigurables , A1.1.13. Virtualisation , A2.2.1. Analyse statique , A2.2.5. Environnements d'exécution , A2.2.6. GPGPU, FPGA... , A2.2.9. Sécurité par la compilation , A2.4.3. Preuves , A2.6.1. Systèmes d'exploitation , A2.6.3. Machines virtuelles , A4.1.2. Attaques sur les équipements , A4.4. Sécurité des équipements et des logiciels , A4.5. Méthodes formelles pour la sécurité , A4.9.1. Détection d'intrusion , A4.9.3. Réaction aux attaques

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : B6.5. Systèmes d'information , B6.6. Systèmes embarqués

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

Période : 01/01/2024 -> 31/12/2027
Dates d'évaluation :

Etablissement(s) de rattachement : CENTRALESUPELEC, ENS RENNES
Laboratoire(s) partenaire(s) : IRISA (UMR6074)

CRI : Centre Inria de l'Université de Rennes
Localisation : Centre Inria de l'Université de Rennes
Code structure Inria : 031140-0

Numéro RNSR : 202424468W
N° de structure Inria: SR0951JR

Présentation

Les systèmes informatiques s'appuient sur des plateformes de calcul pour exécuter les applications des utilisateurs et héberger leurs données. Ces plateformes de calcul sont composées de différents matériels et logiciels systèmes et tendent à devenir de plus en plus complexes. Cette complexité croissante des interactions entre les composants logiciels et matériels soulève des problématiques majeures en termes de confidentialité et de confiance dans les systèmes informatiques actuels. Pour répondre à ces enjeux, l'objectif principal de recherche de l'équipe SUSHI sera d'évaluer et d'augmenter le niveau de sécurité des plateformes de calcul existantes et futures à l'interface matériel/logiciel. Nos objectifs sont notamment :

- d'identifier de nouvelles vulnérabilités résultant des interactions entre logiciels et matériels dans ces plateformes complexes et hétérogènes ;
- de proposer des approches sécurisées par conception pour prévenir l'exploitation de ces vulnérabilités ;
- de développer des approches de détection et de réaction aux intrusions basées sur l'hôte en exploitant les interactions entre logiciels et matériels ;
- de prouver formellement les propriétés de sécurité mises en œuvre par les mécanismes de sécurité matériel/logiciel.

Nous proposons d'articuler nos recherches autour de trois niveaux différents à l'interface matériel/logiciel :

1. **Le niveau de l'architecture et de la micro-architecture matérielle** se concentre sur la partie matérielle de l'interface, qui doit fournir aux logiciels les services nécessaires pour garantir la sécurité ;
2. **Le niveau des logiciels systèmes** cible les logiciels bas-niveau, tels que les systèmes d'exploitation ou les hyperviseurs, qui sont étroitement liés aux interfaces matérielles et doivent les utiliser correctement pour assurer la sécurité ;
3. **Le niveau de l'analyse et de l'instrumentation des exécutables binaires** se concentre sur l'analyse et la modification des exécutables binaires, c'est-à-dire des séquences d'instructions appartenant à

Contact

- **Responsable :** Guillaume Hiet
- **Tél :** 06.50.75.31.36
- **Secrétariat Tél :** 02.99.84.25.77

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2024

Documents sur la structure

- Intranet
- Privés

Décisions

- 16602 (22/11/2023) : création

Localisation

- **Adresse postale :** Centre Inria de l'Université de Rennes 263, avenue du Général Leclerc Campus universitaire de Beaulieu 35042 Rennes Cedex France
- **Coordonnées GPS :** 48.116, -1.64

l’architecture du jeu d’instructions (ISA).

Axes de recherche

- Identification des vulnérabilités et sécurité par conception
- Sécurité réactive au niveau de l’hôte
- Modèles formels et preuves pour la sécurité bas-niveau

Relations industrielles et internationales

- Collaboration avec l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI)
- Collaborations industrielles avec THALES, HP Labs
- Collaboration avec le CEA (PEPR cybersécurité)
- Financements de thèses et collaborations avec la DGA