Application BASTRI
Fiches Equipes

PIRAT (SR0958BR)

Protection de l’information et résistances aux attaques
CIDRE (SR0450UR) PIRAT

Statut: Décision signée

Responsable : Valerie Viet Triem Tong

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : A1.2.2. Supervision , A1.2.8. Sécurité des réseaux , A1.3.3. Blockchain , A1.3.4. Pair à pair , A2.2.1. Analyse statique , A4.1. Analyse de la menace , A4.4. Sécurité des équipements et des logiciels , A4.9. Supervision de la sécurité , A4.9.1. Détection d'intrusion , A4.9.2. Corrélation d'alertes , A4.9.3. Réaction aux attaques , A9.1. Connaissances , A9.2. Apprentissage , A9.6. Aide à la décision , A9.8. Raisonnement , A9.9. IA distribuée, multi-agents , A9.10. Approches hybrides de l'IA

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : B6.5. Systèmes d'information , B9.5.1. Informatique , B9.10. Confidentialité, vie privée

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

Période : 01/03/2024 -> 29/02/2028
Dates d'évaluation :

Etablissement(s) de rattachement : CENTRALESUPELEC, CNRS, U. 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 : 031144-0

Numéro RNSR : 202424530N
N° de structure Inria: SR0958BR

Présentation

L'équipe **PIRAT** (Protection de l’Information et Résistance aux ATtaques) se consacre à la recherche en **cybersécurité**, en particulier à la défense contre les cyberattaques. Notre objectif principale est de comprendre, détecter, et résister aux menaces informatiques en proposant des approches combinant **intelligence artificielle**, **analyse de code**, modélisation, et **systèmes distribués**.

Axes de recherche

1. **Compréhension des attaques** :
    - Analyser les attaques, en reposant sur les traces laissées par l'attaquant: malware, logs système, trafic réseau pour modéliser le comportement de l'attaquant et mettre en évidence des scénarios d'attaques.
    - Collecter des données d'attaques représentatives.
2. **Détection des menaces** :
    - Concevoir des systèmes de détection d'intrusions (IDS) basés sur des approches collaboratives et intelligentes.
    - Exploiter des techniques d'**IA explicable** (XAI) et des systèmes distribués pour améliorer la précision et réduire les faux positifs.
3. **Résilience et réponse aux attaques** :
    - Développer des **cyber-ranges automatisés** pour tester et renforcer la résilience des systèmes critiques.
    - Élaborer des stratégies pour limiter l'impact des attaques et assurer une reprise rapide des opérations.

Relations industrielles et internationales

Contact

- **Responsable :** Valerie Viet Triem Tong
- **Tél :** 02. 9.9 .84. 4.5 .00
- **Secrétariat Tél :** 02. 9.9 .84. 4.5 .00

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 16850 (26/02/2024) : 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