SUJET DE THESE

SUJET : Etude de mécanismes de restauration autonomes pour les systèmes embarqués

DOMAINE DE RECHERCHE : Sécurisation des objets interconnectés

RÉSUMÉ

Le déploiement à grande échelle d'objets communicants au sein de nos systèmes de la vie quotidienne et des infrastructures industrielles, y compris les plus critiques, est accompagné de risques avérés et à venir en matière de cybersécurité. Ce contexte, porteur de défis, nécessite d'améliorer la résilience des objets connectés en anticipant les futures menaces, en améliorant leur résistance aux attaques et en garantissant leur réparation après une tentative d'attaque. Ces fonctions sont considérées par le NIST comme prioritaires pour obtenir un système sécurisé. Si les sujets autour des mécanismes de protection ou de détection de menaces sont actuellement bien couverts, la réparation après attaque est encore peu présente dans la littérature scientifique.

L'objectif de cette thèse est d'identifier des solutions permettant de restaurer les fonctions ou tâches critiques d'un dispositif embarqué après la détection d'un événement non désiré (dû à une malveillance ou bien une défaillance logicielle ou matérielle). Depuis une vingtaine d'années, de nombreux travaux de recherche se sont focalisés sur la définition de solutions de restauration dans le domaine de la sûreté [1], [2], [3], l'application de ces techniques au domaine de la sécurité est plus récente, et encore peu de travaux adressent l'applicabilité de ces méthodes à ce domaine [3][5].

Si les principes de restauration peuvent être identiques dans les domaines de la sûreté et de la sécurité, dans le cas d'action malveillante, il est en plus nécessaire de rendre le système de restauration robuste contre des tentatives de corruption par l'attaquant. En effet, celui-ci peut faire évoluer son attaque afin de leurrer le système de restauration ou bien même corrompre la restauration elle-même. Une des hypothèses de départ pris dans cette thèse est que le système possède déjà un ou plusieurs modules de détection d'événements anormaux. A partir de cet état anormal, la solution doit permettre la restauration du logiciel après avoir vérifié l'intégrité du bloc logiciel défaillant (rollback) grâce à une sauvegarde du contexte (checkpoint) à intervalles réguliers. Dans le cadre de cette thèse, l'étude portera uniquement sur les processeurs intégrant un OS de type Linux embarqué mais sa portabilité vers d'autres OS pourra être analysée.

Cette thèse doit permettre de lever un certain nombre de verrous concernant l'applicabilité de la restauration des systèmes dans le domaine sécuritaire :

Il est nécessaire en premier lieu d'apporter des garanties quant à la confiance que l'on peut avoir dans le système de restauration (au moment de la conception du système et lors de l'exécution).

- On s'intéressera ainsi à la sécurisation intrinsèque des mécanismes de restauration :
    - La sauvegarde de contexte et sa restauration sont les fonctions les plus critiques du système et ne doivent pas être la cible de l'attaque ou être utilisée pour mener une attaque. La connaissance des mécanismes développés par un attaquant ne doit pas permettre à celui-ci de modifier le comportement de son

système afin de contourner la protection. La solution proposée doit prendre en compte cette contrainte.
    - Avec l'apparition de cœurs intégrant des mécanismes de sécurité d'isolation matérielle (ex : ARM Trustzone), l'impact de ces nouvelles architectures sur les solutions développées devra être considéré.

- Des méthodes de validation pourront aussi être mises en place dès la conception pour valider l'efficacité sécuritaire de la solution tout en minimisant son impact sur le reste des paramètres fonctionnels :
    - En sureté, des outils de type FMEA (Fault Mode and Effects Analysis) permettent d'automatiser la détection des fautes dans le flux de contrôle et d'identifier les points d'intérêt et de préparer la phase de validation de la solution [2]. Des modèles et outils de fautes existent également dans le contexte de la sécurité et pourront être utilisés dans le cadre de notre analyse.
    - Les stratégies fail-safe et fail-secure décrivent le comportement d'un système en cas de panne. En fonction du ou des scénarios d'usage définis avec des industriels, il sera nécessaire d'assurer que les fonctions les plus critiques ne soient pas impactées par la solution mise en place et qu'elles soient toujours opérationnels, même au détriment de fonctions moins prioritaires.

Enfin, pour faciliter l'acceptation de ces méthodes, leur impact au niveau système doit être minimal :

- Passage à l'échelle :
    - Dans un premier temps on étudiera des systèmes autonomes puis on étudiera l'applicabilité de l'approche dans des systèmes distribués (en particulier l'approche semble adaptée dans le cas des systèmes distribués type multi agent).
- Optimisation de la solution :
    - Une telle solution n'est viable que si elle possède un cout faible et un overhead en temps et mémoire faible. Les tests de performances sur cible réelle ou émulée devront permettre de vérifier les optimisations réalisées sur la gestion des sauvegardes.
    - La localisation des checkpoints est un sujet déjà abordée dans l'état de l'art mais devra être consolidée dans le contexte de la sécurité.

Bibliographie :

[1] G. Luan, Y. Bai, C. Wang, J. Zeng and Q. Chen, "An Efficient Checkpoint and Recovery Mechanism for Real-Time Embedded Systems," 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications

[2] J. Arm, Z. Bradac, R. Stohl, Increasing Safety and Reliability of Roll-back and Roll-forward Lockstep Technique for Use in Real-time Systems, 2016

[3] Bashiri, Mohsen & Miremadi, Seyed Ghassem & Fazeli, Mahdi. (2007). A Checkpointing Technique for Rollback Error Recovery in Embedded Systems. 174 - 177. 10.1109/ICM.2006.373295.

[4] Wang, X.; Zhao, Z.; Xu, D.; Zhang, Z.; Hao, Q.; Liu, M.; Si, Y. Two-Stage Checkpoint Based Security Monitoring and Fault Recovery Architecture for Embedded Processor. Electronics 2020, 9, 1165. https://doi.org/10.3390/electronics9071165

[5] Ronny Chevalier, David Plaquin, Chris Dalton, Guillaume Hiet. Intrusion Survivability for Commodity Operating Systems. Digital Threats: Research and Practice, Association for Computing Machinery, 2020

Qualifications requises

- Diplôme d'ingénieur ou Master 2
- Bonnes capacités de prototypage rapide (maitrise d'un langage adapté tel que Python)
- Compétences reconnues en développement logiciel embarqué (C, OS embarqués, drivers, assembleur, etc.) ; principalement en Linux Embarqué
- Perception des spécificités de la sécurité appliquée aux systèmes embarqués
- Connaissance des outils et techniques de Pentesting
- Curiosité et volonté de comprendre le fonctionnement des systèmes
- Langues : français, anglais

Cadre du travail

Le département Système du CEA (Commissariat à l'Energie Atomique et aux Energies Alternatives) opère un service en charge de la Sécurité des Systèmes Electroniques et des Composants (SSSEC), acteur majeur de l'activité et de l'offre sécurité globale du CEA-Leti. Ce service intervient en particulier sur l'évaluation des vulnérabilités et la conception de technologies et de systèmes sécurisés, sur des domaines applicatifs en très forte croissance. Au sein de ce service, le Laboratoire Systèmes Embarqués Sécurisés (LSES) intervient plus particulièrement sur la conception et l'intégration de technologies de sécurité dans les systèmes embarqués et autres objets connectés, et ce sur divers domaines applicatifs tels que l'IoT/IIoT/IoMT, l'Energie, l'Automobile, la Santé et la Smart City.

Informations complémentaires :

- Localisation : Grenoble
- Encadrants : Pierre-Henri Thevenon, Maxime Puys
- Directrice de thèse : Oum-El-Kheir Aktouf
- Durée : 36 mois (à partir du 01/07/2023)