Titre de la thèse : Fine-grained data-flow security in real-time critical systems (FILTRATE)

Contact : Alain Plantec (alain.plantec@univ-brest.fr), Hai Nam Tran (hai-nam.tran@univ-brest.fr)
Établissement d'accueil : Université de Bretagne Occidentale (https://www.univ-brest.fr/)
Unité de recherche : Lab-STICC (https://www.labsticc.fr/)

Mots clés : Sécurité, Vérification, Modélisation, Systèmes temps réel embarqués

Profil et compétences recherchées :
- Le/la doctorant(e) devrait préférablement avoir une formation ou une première expérience dans l'un des domaines suivantes :
    + Système temps-réel
    + Architectures embarquées
    + Modélisation, c'est-à-dire connaissance des langages et outils de modélisation
- Les compétences en cybersécurité et génie logiciel sont appréciées

Descriptif de la thèse

Les méthodes de validation les plus utilisées pour les systèmes temps réel critiques visent à garantir leurs propriétés temporelles. Cependant, face aux cyberattaques, ces méthodes sont inopérantes pour garantir le bon fonctionnement d'un système en cours d'exploitation. Les travaux menés pour cette thèse visent à garantir la bonne exécution d'un système par un contrôle dynamique des opérations effectuées sur les données et de leur ordonnancement.

Contexte : La thèse porte sur la cybersécurité dans les systèmes temps réel critiques. La validité de ces systèmes ne dépend pas seulement des valeurs des résultats produits, mais également des délais dans lesquels les résultats sont produits. Ils sont qualifiés de critiques car la défaillance d'un tel système a des conséquences inacceptables pour la société. De tels systèmes se composent de différentes tâches qui peuvent s'exécuter simultanément ou en séquence et peuvent être synchronisées suivant un ordonnancement contrôlé. Ils sont, par exemple, mis en œuvre pour les véhicules autonomes, les véhicules aériens sans pilote (UAV), ou les robots. Leur vérification repose actuellement en grande partie sur la validation des propriétés temporelles. Le concepteur dispose d'informations précises concernant ces propriétés qui peuvent être soit exprimées par modélisation, soit produites par analyse d'ordonnancement.

Problématique : Les méthodes les plus utilisées pour valider de tels systèmes visent notamment à garantir leurs propriétés temporelles. Ces méthodes de validation sont qualifiées de *précoces* car elles sont utilisées pendant la phase de conception des systèmes. Cependant, face à des dysfonctionnements matériels, des dysfonctionnements logiciels ou des attaques malveillantes, la validation précoce des propriétés temporelles est insuffisante pour garantir le bon fonctionnement d'un système en cours d'exploitation. En effet, à tout moment, un flux de données peut être corrompu à cause d'altérations imprévues.

Par exemple, un dysfonctionnement ou une attaque avec intrusion agissant par remplacement de certains composants peuvent conduire :
- à un retard des accès aux données (cf. Figure 1a),
- à des modifications de l'ordre des accès aux données (cf. Figure 1b),
- ou à des absences d'accès aux données (cf. Figure 1c).

Il faut donc être capable de mesurer le décalage temporel éventuel des accès aux données, de contrôler leur nature et de détecter l'ajout ou la suppression de certains accès aux données.

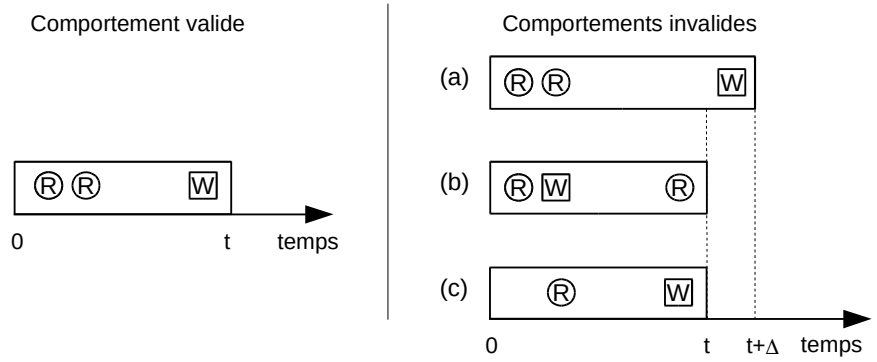

Figure 1 : Exemple de détections des comportements invalides en prenant en compte des opérations effectuées sur les données

Objectifs généraux : Les travaux menés pour cette thèse visent à accroître les capacités de vérification du fonctionnement d'un système par un contrôle dynamique des opérations effectuées sur les données et de leur ordonnancement : il s'agit donc de contrôler pendant l'exécution du système, que les opérations effectuées sur les données demeurent conformes à ce qui a été prévu par le concepteur.

En cours de fonctionnement, on peut considérer un système temps réel comme un graphe d'éléments qui interagissent par échange de données. À tout moment, une donnée peut être altérée. La cause d'une telle altération peut être un dysfonctionnement matériel ou logiciel ou encore la résultante d'une attaque malveillante. Des études récentes ont montré qu'il existe différentes possibilités d'attaque, notamment les attaques matérielles pures, les attaques par les réseaux sans fil et les attaques par altération des mécanismes de captation des données par les capteurs.

Pour ces travaux les questions soulevées sont les suivantes:

a) Comment qualifier les données en tenant compte du temps ?
b) Comment contrôler qu'une opération effectuée sur des données est valide à un moment donné ?
c) Comment contrôler l'absence ou la présence non anticipée de certains accès aux données ?
d) Comment instrumenter la mise en œuvre des systèmes temps réel avec des techniques de contrôle des opérations effectuées sur les données ?
e) Comment améliorer les simulateurs pour mettre en évidence les déficiences possibles ?

Dans un système temps réel, le contrôle de l'ordre d'exécution des tâches est assuré par un ordonnanceur qui s'appuie sur les propriétés temporelles des tâches qu'il gère. Classiquement, un ordonnanceur applique un modèle d'ordonnancement des tâches qui a été validé pendant la conception du système. L'ordonnanceur dispose donc d'un point de vue global sur l'ensemble du système en cours d'exécution : les tâches qui s'exécutent et leurs propriétés temporelles. L'idée directrice de cette thèse est d'étudier comment exploiter l'ordonnanceur et le modèle temporel qu'il est censé appliquer pour un contrôle dynamique des opérations effectuées sur les données.

Travail attendu : Les travaux s'appuieront sur des travaux préliminaires pour proposer une méthode de modélisation des relations entre les opérations effectuées sur les données, les tâches du système et les propriétés temporelles – les relations « temps-données ». En d'autres termes, nous visons à créer des modèles de tâches enrichis pour l'analyse de systèmes temps réel critiques en prenant en compte les opérations effectuées sur les données. Ces modèles seront ensuite utilisés pour atteindre les deux contributions suivantes.

Contribution 1 : *Conception de composants dédiés à la surveillance et au contrôle des accès aux données*. Développement de nouveaux patrons de gestion de données associées à des extensions

d’un langage de modélisation temps réel (comme AADL) permettant le contrôle et l'autorisation des injections, des lectures et des modifications en fonction du temps et des tâches pour par exemple interdire à une tâche de modifier une donnée pendant une période non autorisée ou détecter l’absence de certains accès aux données.

Contribution 2 : *Simulation d'ordonnancement.* Il est nécessaire de disposer d’un outil de simulation permettant de valider les composants dédiés à la surveillance des données et notamment, leurs propriétés temporelles. Cet outil devrait permettre non seulement de simuler les accès aux données, mais aussi d’introduire dynamiquement des perturbations pour mettre à l’épreuve le système.

La thèse se déroulera dans le cadre du projet Cheddar. Ce projet, initié en septembre 2000 au Lab-STICC, a pour objectif d'accroître l'applicabilité de la théorie de l'ordonnancement temps réel. Dans ce projet, nous étudions comment un langage de conception d'architecture peut contribuer à faciliter la vérification des performances d'un système temps réel critique avec la théorie de l'ordonnancement temps réel. Cette activité est conduite dans le cadre d'un partenariat avec la société *Ellidiss Technologies* située sur Brest. Les travaux menés durant cette thèse permettront d'élargir les contributions du projet Cheddar concernant la validation dynamique et la sécurisation des systèmes temps-réel critiques.