CYBERSIM : Automatisation de l'appréciation du risque de cybersécurité via des scénarios d'attaque

Mike Da Silva*, Nga Nguyen†
De Vinci Higher Education, Research Center
92 916 Paris La Défense, France
prénom.nom@devinci.fr

I. Contexte

Pré-CYBERSIM est un postdoctorat financé par le Programme de Transfert au Campus Cyber (PTCC), labellisé France 2030, en collaboration avec Airbus Protect pour une durée de 1 an. Ce projet, qui a démarré en octobre 2024, a pour objectif d'automatiser conjointement les analyses de sûreté et de cybersécurité dans un même outil : le logiciel SimfiNeo développé par Airbus Protect. Les résultats permettront d'automatiser les tâches et d'optimiser le temps de travail des analystes des risques pour évaluer les scénarios les plus probables, identifier les faiblesses de l'architecture du système et mettre en œuvre des contre-mesures. Tout cela dès la conception du système, en combinant à la fois des analyses de sûreté et de sécurité dans le même outil.

II. Verrous scientifiques et technologiques

SimfiaNeo utilise le formalisme mathématique des systèmes d'événements discrets, via le langage AltaRica [Arnold2000], qui fournit une modélisation du comportement du système sous forme de séquences d'événements conduisant à un état critique. Ces séquences permettent d'identifier les faiblesses du système étudié et donnent des pistes d'amélioration de son architecture pour remédier à ces faiblesses. L'enjeu de ce projet est d'adapter ce formalisme des systèmes d'événements discrets initialement dédié à la sûreté afin d'intégrer la sécurité et ainsi pouvoir analyser conjointement la sûreté et la sécurité dans SimfiaNeo. Une étude préalable sur les points communs et les différences entre les séquences critiques dans le domaine de la cybersécurité (cyberattaques) et celui de la sûreté (défaillances) [Serru2023] observe deux différences majeures qui nécessitent des adaptations pour appliquer le formalisme des systèmes d'événements discrets au domaine de la cybersécurité.

Premièrement, les séquences critiques représentant les cyberattaques ont tendance à être plus longues que celles représentant les défaillances, ce qui aggrave le problème d'explosion combinatoire caractéristique des systèmes cyber-physiques. Deuxièmement, les séquences critiques pour la sûreté sont des combinaisons de défaillances indépendantes dont l'ordre n'a pas d'importance, contrairement aux cyberattaques qui sont une suite d'actions intentionnelles dans le but d'atteindre un objectif défini.

Une première contribution a été de proposer des critères de coupure comme des « empreintes » qui prennent en compte les dépendances entre les actions d'un attaquant pour réduire le nombre de séquences générées. Des résultats préliminaires obtenus avec un cas d'étude (architecture automobile extraite du projet [EVITA2011]) ont permis de passer de 401 625 séquences de longueur 10 à 72 séquences avec une empreinte inférieure ou égale à 2, réduisant le temps de calcul de 14 minutes à moins d'1 seconde. Cependant, cette approche ne permet d'évaluer la pertinence (sévérité) des séquences générées et nécessite d'identifier comment adapter un cadre formel initialement dédié à la sûreté, qui traite d'événements aléatoires et non intentionnels en utilisant des méthodes statistiques, à la sécurité, avec des menaces intentionnelles pour lesquelles des statistiques pertinentes ne peuvent généralement pas être définies par manque de données statistiques fiables sur le nombre et les fréquences d'attaques dans le temps pour calculer des distributions probabilistes représentatives de la réalité.

III. Pistes de recherche

En plus du critère d'empreinte, nous étudions des analyses quantitatives avec des métriques de sécurité telles que le coût ou la vraisemblance d'une attaque selon différents profils d'attaquants, afin de classifier les séquences générées selon leur pertinence. Cela aura pour effet de pouvoir filtrer les séquences de moindre importance et de concentrer les efforts sur les faiblesses les plus critiques du système. Plus précisément, nous souhaitons :

1) Établir un modèle de coûts flexible et adapté aux différents contextes et aux données disponibles, en proposant des fonctions d'agrégation appropriées pour les scénarios d'attaque (séquences) ;
2) Appliquer ce modèle sur un cas d'étude industriel et le faire valider par des analystes des risques en cybersécurité.

Le postdoctorat Pré-CYBERSIM actuellement en cours vise à proposer une preuve de concept (TRL 3) du modèle de coût qui sera, dans la suite du projet, porté TRL 4 à 5.

*Intervenant, †Porteuse du projet

RÉFÉRENCES

[Arnold2000] André Arnold, Alain Griffault, Gérald Point, and Antoine Rauzy. The AltaRica language and its semantics. Fundamenta Informaticae, 34 :109–124, 2000

[Serru2023] Théo Serru, Nga Nguyen, Michel Batteux, and Antoine Rauzy. 2023. Minimal Critical Sequences in Model-based Safety and Security Analyses : Commonalities and Differences. ACM Trans. Cyber-Phys. Syst. 7, 3, Article 17 (July 2023), 20 pages. https ://doi.org/10.1145/3593811

[EVITA2011] EVITA Project. 2011. EVITA : E-safety vehicle intrusion protected applications. https://www.evita-project.org/