Approche Dirigée par les Modèles pour la Sécurité Auto-adaptative des Systèmes Cyber-physiques

Salim Chehida, Eric Rutten, Guillaume Giraud, Stéphane Mocanu

Approche Dirigée par les Modèles pour la Sécurité Auto-adaptative des Systèmes Cyber-physiques

Salim Chehida[1], Eric Rutten[1], Guillaume Giraud[2], Stéphane Mocanu[1]

[1]*Univ. Grenoble Alpes, Inria, CNRS, Grenoble INP, LIG, Grenoble*
[2]*RTE, Paris*

Résumé

Ce travail propose approche pour la sécurité auto-adaptative dans les systèmes cyber-physiques (CPS) : architecture logicielle, méthode de conception, intégration avec la prise de décision basée sur les modèles. Notre approche permet l'évaluation du risque de sécurité (SRA), en tenant compte les aspects de qualité de service (QoS). Nous formalisons le problème de décision à résoudre à chaque cycle de la boucle de contrôle d'auto-adaptation en termes de modélisation et de résolution par programmation de contraintes (CP). Nous validons notre approche en l'appliquant aux réseaux électriques intelligents, plus particulièrement à une étude de cas industrielle fournie par RTE, le gestionnaire du réseau de transport d'électricité français.

Ce document est un résumé long de l'article suivant :

Salim Chehida, Eric Rutten, Guillaume Giraud, Stéphane Mocanu, *A model-based approach for self-adaptive security in CPS: Application to smart grids*, Journal of Systems Architecture, Volume 150, 2024, 103118, ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2024.103118.

1 Introduction

L'évaluation des risques de sécurité est un défi majeur dans la conception des CPS. La nature intrinsèquement dynamique de ces systèmes, due aux changements dans leur environnement ainsi qu'aux évolutions de leurs infrastructures, les rend des systèmes auto-adaptatifs, où les aspects de sécurité doivent être pris en compte en termes de gestion des détections et des réactions pour l'auto-protection. Dans les CPS auto-adaptatifs, une séquence de reconfigurations est effectuée à l'exécution pour faire face aux changements de besoins et d'environnement. Cette adaptation garantit la fonctionnalité et la qualité, mais expose également de plus en plus le système à des actes malveillants. Les attaquants peuvent sélectionner la configuration la plus vulnérable pour augmenter leurs chances de succès. Ainsi, une évaluation des risques de sécurité dans le processus d'adaptation est fortement nécessaire. Les menaces et les vulnérabilités de chaque configuration doivent être analysées afin d'identifier les défenses pertinentes qui minimisent les chances de l'attaquant et garantissent un bon niveau de sécurité. Par conséquent, l'influence des configurations de défense sur le système doit être évaluée afin de maintenir une bonne qualité de service. Cela appelle à l'intégration de mécanismes d'auto-protection avec les autres aspects tels que les ressources et la qualité de service, dans une gestion complète de l'auto-adaptation.

Dans ce travail, nous proposons l'intégration de sécurité auto-adaptative en tenant compte de la séparation des préoccupations dans le contrôle respectif des niveaux d'application et d'infrastructure en se basant sur des travaux antérieurs [3], et nous fournissons également un mécanisme de coordination entre les deux niveaux en évaluant les reconfigurations qui améliorent la qualité de service. La Figure 1 montre le shéma général de notre approche. Nous considérons un ensemble de modes d'application (configurations fonctionnelles) et un ensemble de modes d'infrastructure (configurations architecturales) du système. Le mécanisme de contrôle de sécurité auto-adaptatif récupère les modes d'application et

d'infrastructure actuels. Ensuite, en fonction des menaces détectées, il fournit un ensemble de configurations sécurisées pour atténuer les risques identifiés. Chaque configuration sécurisée active un ensemble de réactions qui garantissent un certain niveau de sécurité et des contraintes de QoS, puis la configuration sécurisée à haute performance est sélectionnée tout en trouvant un équilibre entre la sécurité et la QoS. Notre approche comprend deux phases. Nous commençons par modéliser les menaces et les réactions de l'ensemble du système dans la Section 2. Ensuite, nous construisons le mécanisme de sécurité auto-adaptatif qui prend en compte les risques de sécurité et les contraintes de QoS dans la Section 3.

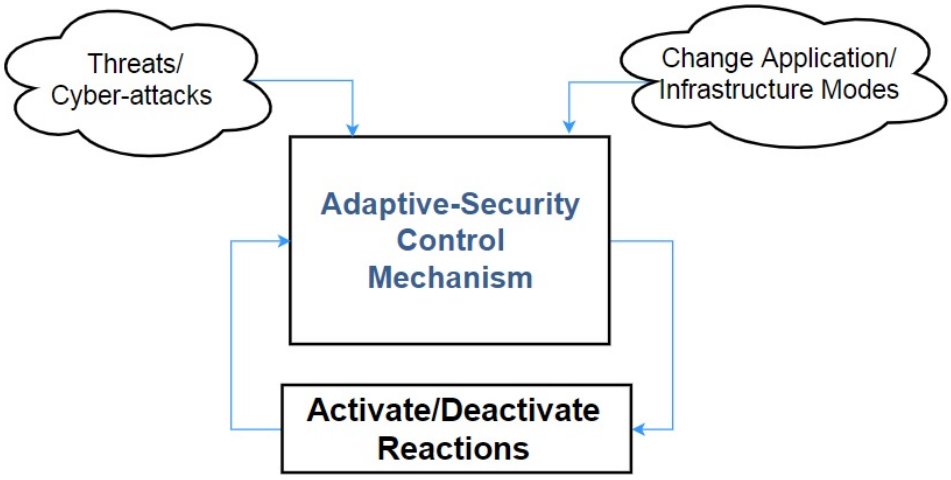

Figure 1: Approche d'auto-protection

2 Modélisation des menaces et des réactions

Dans ce travail, nous suivons une approche basée sur les Arbres Attaque-Défense (ADT) et la méthodologie d'évaluation des risques de sécurité BRAIN-IoT [1] développée dans le cadre du projet européen BRAIN-IoT[1]. Comme le montre la Figure 2, les principales étapes de notre approche d'évaluation des risques de sécurité sont :

1. Nous spécifions les différents actifs du système. La norme ISO/IEC 27001 définit un actif comme "toute chose tangible ou intangible ou toute caractéristique ayant de la valeur pour une organisation".

2. Nous identifions les menaces pesant sur tous les actifs du système en nous basant sur les bases de données des menaces courantes proposées par les normes de sécurité. Dans ce travail, nous utilisons la classification STRIDE et la base de données générique ISO/IEC 27005 pour sélectionner les menaces pertinentes.

3. Nous spécifions les réactions qui peuvent être déployées dynamiquement sur l'infrastructure pour défendre le système contre les menaces identifiées. Les réactions que nous considérons représentent des actions de sécurité qui peuvent être activées ou désactivées à l'exécution.

4. Nous construisons l'ADT en combinant les menaces et les réactions. L'ADT est un arbre raciné qui comprend des nœuds de deux types opposés : les nœuds de menace et les nœuds de réaction. Les combinaisons entre les nœuds peuvent être exprimées par des opérateurs logiques. Dans ce travail, nous utilisons l'outil ADTool [2] pour modéliser l'Arbre Attaque-Défense

[1] https://www.brain-iot.eu/

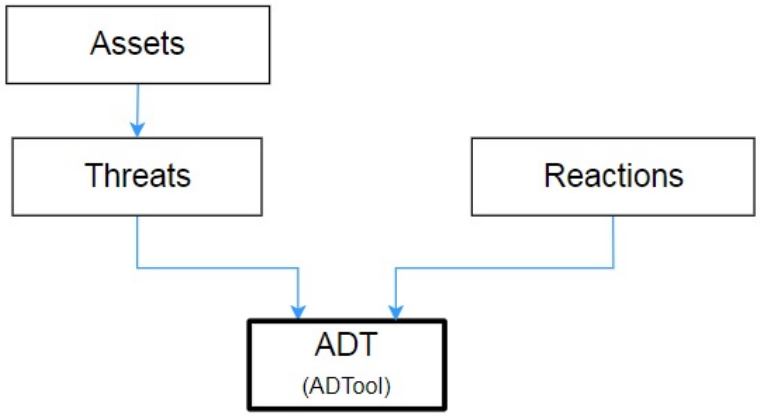

Figure 2: Approche de modélisation des menaces et des réactions

3 Conception du mécanisme de sécurité auto-adaptatif

Le système de contrôle de sécurité auto-adaptatif est construit à partir de l'ADT. Nous suivons une approche décisionnelle basée sur un modèle pour la conception de notre mécanisme de sécurité auto-adaptatif.

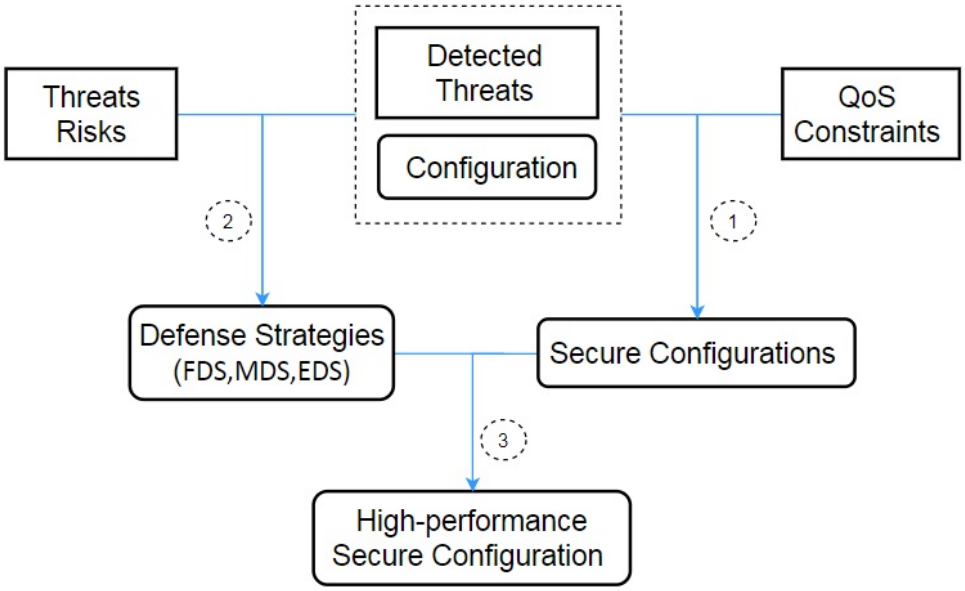

Figure 3: Étapes de conception du mécanisme de contrôle de sécurité auto-adaptatif

Comme le montre la Figure 3, nous suivons trois étapes :

1. Nous définissons les configurations sécurisées qui activent l'ensemble des réactions permettant de bloquer les menaces détectées d'une configuration donnée, tout en respectant les contraintes de QoS.

2. Nous classifions les menaces détectées d'une configuration donnée (combinaison d'application et d'infrastructure) en fonction de leur niveau de risque, par exemple : élevé, moyen et faible. Ensuite, nous définissons un ordre décroissant de sous-ensembles de ces menaces. Le premier sous-ensemble TS1 inclut toutes les menaces de configuration détectées, le deuxième TS2 exclut les menaces à faible risque, et le troisième sous-ensemble TS3 inclut uniquement les menaces à haut risque. Enfin, nous définissons des stratégies de défense en sélectionnant les réactions qui

peuvent bloquer les sous-ensembles de menaces. La FDS (Stratégie de Défense Complète) bloque TS1. La MDS (Stratégie de Défense de Niveau Moyen) bloque TS2. La EDS (Stratégie de Défense Essentielle) bloque TS3. Chaque stratégie garantit un certain niveau de sécurité.

3. Nous sélectionnons la configuration sécurisée qui correspond à la meilleure stratégie de défense et garantit le niveau de QoS nécessaire.

4 Implémentation et application

Dans ce travail, nous utilisons une approche basée sur la Programmation par Contraintes (CP) pour concevoir le contrôleur de sécurité auto-adaptatif. Le modèle CP implémente un ensemble de contraintes formelles permettant de spécifier des configurations sécurisées, évaluées en fonction de leur impact sur les performances du système afin de déterminer la plus pertinente représentant un bon équilibre entre la sécurité et la qualité de service. Six équations de contraintes ont été spécifiées pour exprimer les configurations de l'application et de l'infrastructure (C1), les configurations sécurisées (C2), les objectifs de qualité de service (C3), et les différentes stratégies de défense FDS (C4), MDS (C5), et EDS (C6).

Nous avons implémenté notre modèle CP en utilisant l'outil IBM ILOG CPLEX Optimization Studio[2]. Le code pour la simulation a été écrit en langage OPL, et les problèmes ont été résolus par la version 12.8.0 de CPLEX.

Nous avons appliqué notre approche à l'étude de cas industrielle du réseau de transmission électrique intelligent de la zone de Melle-Longchamp de RTE. Le système RTE se compose de différents modes d'adaptation d'application et d'infrastructure. Nous avons utilisé notre approche pour analyser les risques de sécurité de chaque reconfiguration combinant des modes d'application et d'infrastructure. Ensuite, en fonction de la configuration actuelle, des menaces détectées et des contraintes de performance, la configuration sécurisée appropriée activant un ensemble de réactions pertinentes sera identifiée et exécutée. Nous avons effectué différents scénarios de reconfiguration qui ont confirmé que le système était capable de gérer les menaces de sécurité émergentes tout en maintenant la meilleure qualité de service possible.

5 Conclusion

Nous avons présenté une approche pour construire des mécanismes de sécurité auto-adaptatifs des CPS. Notre solution prend en compte la séparation des préoccupations entre les niveaux d'application et d'infrastructure et analyse les menaces associées à chaque combinaison de ces niveaux. Elle utilise ensuite la résolution de contraintes pour fournir une décision de reconfiguration de sécurité optimale qui permet d'une part de maximiser la QoS et d'autre part de maximiser la réponse aux menaces de sécurité.

References

[1] Chehida, S., Baouya, A., Alonso, D.F., Brun, P.E., Massot, G., Bozga, M., Bensalem, S.: Asset-driven approach for security risk assessment in iot systems. In: Garcia-Alfaro, J., Leneutre, J., Cuppens, N., Yaich, R. (eds.) Risks and Security of Internet and Systems. pp. 149–163. Springer International Publishing, Cham (2021)

[2] Kordy, B., Kordy, P., Mauw, S., Schweitzer, P.: Adtool: Security analysis with attack–defense trees. In: Joshi, K., Siegle, M., Stoelinga, M., D'Argenio, P.R. (eds.) Quantitative Evaluation of Systems. pp. 173–176. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)

[3] Tourchi Moghaddam, M., Rutten, E., Giraud, G.: Hierarchical Control for Self-adaptive IoT Systems A Constraint Programming-Based Adaptation Approach. In: HICSS 2022 - Hawaii International Conference on System Sciences. pp. 1–10. Hawaii, United States (Dec 2022)

[2] https://www.ibm.com/products/ilog-cplex-optimization-studio