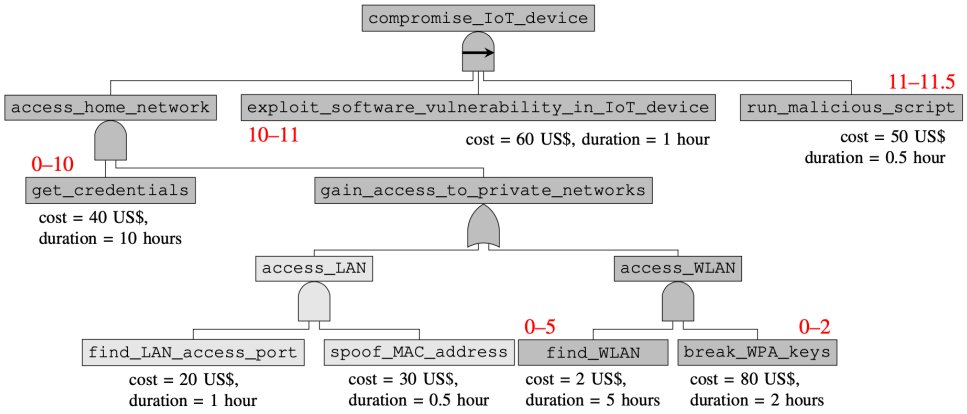
Encadrant : M. Ramparison (mathias.ramparison@grenoble-inp.fr)

10 December 2021

Calculs et optimisation dans les arbres d'attaque et de défaillance

Contexte : sureté et sécurité des systèmes cyber-physiques.

Introduction : avec l'utilisation de plus en plus complexe des infrastructures informatiques, logicielles et matérielles, l'analyse des systèmes cyber-physiques devient de plus en plus technique et doit prendre en compte un nombre de contraintes croissant.
Les arbres d'attaque et de défaillance sont un *formalisme simple, haut niveau et compréhensible* par des profils plus ou moins techniques de l'industrie permettant de modéliser des *scénarios* dans lesquels une entité malicieuse tente de compromettre une infrastructure, du matériel ou un logiciel informatique. Un *scénario* est représenté par un ensemble *d'évènements*, produits par l'entité malicieuse elle-même (*attaque*) ou alors indépendants d'une action extérieure (*défaillance*). Ces évènements peuvent être dépendants de *paramètres* comme par exemple du *temps*, de *probabilités*, d'un *coût* budgétaire et sont liés entre eux par des *connecteurs logiques* (ou, et, etc.).
Pour modéliser l'ensemble de ces évènements et leurs liens, le format d'arbre est le plus répandu parmi les utilisateurs académiques et industriels. Les évènements sont représentés par des feuilles et sont reliés entre eux par des connecteurs. La racine de l'arbre représenté en haut modélise l'action finale, la conséquence ultime du scénario (voir exemple ci-dessous, lecture de bas en haut)



Objectif : Le but de ce projet est de réaliser une interface de calcul et d'optimisation des paramètres amenant à un scénario d'attaque ou de défaillance "réussi", c'est à dire que notre système en sort compromis, modélisé par le fait que la racine de l'arbre est atteinte.

Les calculs sont :

- Temps total du scénario d'attaque
- Coût du scénario pour l'attaquant
- Dommages causés à l'infrastructure, en budget
- Probabilité de réussite du scénario

Des calculs sur plusieurs paramètres peuvent être faits simultanément (par exemple, temps et coût).

Ensuite, le but est de pouvoir optimiser les scénarios : quel est le scénario d'attaque le plus rapide avec le coût le moins élevé pour l'attaquant? Existe-il un scénario d'attaque plus long mais qui cause plus de dommages? Quel est le scénario avec la plus haute probabilité de réussite dans un temps limité?

Pour aller plus loin, deux idées sont envisageables :

- réaliser une interface graphique pour créer ses arbres
- apprendre un arbre à partir d'un ensemble de scénarios (monitoring)

Contraintes : Le choix des méthodes d'optimisation est laissé aux étudiants. La représentation des arbres aussi, par exemple un format JSON conviendra. La représentation de l'arbre et celle de ses paramètres doivent être indépendantes : c'est à dire qu'on doit pouvoir laisser des paramètres vides sur des évènements sans perturber les calculs sur les autres paramètres, mais également pouvoir ajouter des "types" de paramètres autres que ceux cités, ainsi que laisser la possibilité de définir les règles de calcul pour ces nouveaux "types" de paramètres.