Stage de Master M1 : Modélisation d'impact opérationnel et optimisation de contremesures

Contexte

Le déploiement de contremesures face à une attaque sur un système d'informations est un enjeu crucial pour la cybersécurité. En effet, le temps écoulé avant la mise en place de contremesures, ainsi que l'efficacité de ces dernières ont un impact majeur sur la progression de l'attaquant et les dégâts causés au système. Dans l'optique d'en automatiser le déploiement, nous souhaitons ainsi optimiser la sélection de contremesures, selon plusieurs critères.

La question de l'impact des attaques et des contremesures sur un système d'information se pose en effet généralement en termes de coût financier. Toutefois, il est essentiel de s'intéresser également à leur impact opérationnel, c'est-à-dire capacité à leur probabilité d'entraver le bon fonctionnement d'une ou plusieurs fonctions métiers. Par exemple, face à une certaine attaque, l'ajout d'une règle sur un firewall pourrait être vu comme étant la meilleure contremesure en termes de coût financier, mais avoir une probabilité importante d'entraver l'exécution normale d'une fonction métier essentielle. L'impact opérationnel permet alors d'élargir le champ d'analyse pour le déploiement optimal de contre-mesures, en fournissant un deuxième critère à prendre en compte.

Encadrant, lieu et date de stage

Encadrant : Christophe Kiennert (christophe.kiennert@telecom-sudparis.eu)

Lieu : Télécom SudParis, département RST (directeur du département : Hervé Debar)

Durée : Début mai à fin août 2020 (possibilité de commencer à distance)

Objectif et finalité du stage

Ce travail s'inscrit dans une contribution au projet H2020 SOCCRATES.

Travail bibliographique : Lecture et restitution de l'article « Selection of Pareto-efficient response plans based on financial and operational assessments », de A. Motzek et al.

Travail théorique et pratique : Etablir une modélisation de l'impact opérationnel par une approche graphique probabiliste. Ce travail devra proposer une méthodologie pour la représentation des dépendances entre équipements techniques et fonctions métier, prendre en compte la propagation des événements dans le système, et proposer une méthodologie d'évaluation des paramètres afin de pouvoir appliquer ce modèle à des cas d'usage réels pour le calcul de l'impact opérationnel d'attaques, mais également pour déterminer des contremesures optimales.