Nouvelles vulnérabilités, nouvelles menaces, nouvelles solutions

Grenoble mardi et mercredi 30 et 31 janvier 2018

Comment modéliser des attaques sophistiquées ?

Jean Caire

Chargé d'expertise au Contrôle général de sécurité – RATP

Tel : 33 6 72 33 58 69 – jean.caire@ratp.fr

Mots clés : *kill chain, lignes d'opération, modèle semi-formel*

Résumé :

Cette communication présente un ensemble de modèles développés ces dernières années et actuellement mis en œuvre sur des systèmes majeurs de la RATP pour identifier puis modéliser des scénarios d'attaque multi-dimensionnels, c'est-à-dire englobant les trois dimensions essentielles d'un système complexe : humaine, cybernétique et physique.

La présentation est divisée en 3 parties

- La première expose un état de l'art synthétique de la modélisation d'attaque issu des doctrines militaires, de la communauté du renseignement et de la criminologie, avec un focus sur certains concepts-clés (e.g. *kill chain*, *crime scripting*) en analysant d'une part leurs forces et faiblesses et en étudiant d'autre part leur application au cyberespace.

- La seconde partie propose un modèle semi-formel d'une grammaire d'attaque – directement inspiré de l'état de l'art précédent – qui permet de construire de manière logique des scénarios détaillés en combinant des modèles-types élémentaires par des règles précises de la forme Préconditions – Postconditions. L'idée de cette grammaire est de combler le vide qui existe aujourd'hui entre la description d'Evénements Redoutés de « niveau stratégique » et les catalogues de *patterns* de niveau tactiques, tels ceux du MITRE (i.e. CAPEC).

- La dernière partie développe un exemple d'application de la grammaire d'attaque sur une architecture générique de système de transport définie à partir des standards IEC du domaine.

Il faut insister sur le fait que ce travail est uniquement fondé sur des données publiques.