Détection Effective de Portes Dérobées Logicielles

Michaël Marcozzi*[1]

[1]CEA LIST – Commissariat à l'énergie atomique et aux énergies alternatives – France

Résumé

Les logiciels étant le moteur d'une part croissante des activités humaines, ils sont continuellement attaqués à des fins criminelles, économiques, politiques et stratégiques. Les attaquants essaient de se faufiler dans les programmes afin de voler des données, de détourner des processus et de perturber des activités. Pour ce faire, ils peuvent notamment exploiter des portes dérobées pour atteindre leurs objectifs. Une porte dérobée est une fonctionnalité de programme cachée par un développeur malveillant ou négligent et implémentant une faille de sécurité, comme un accès secret. Elles sont particulièrement inquiétantes car la pratique actuelle voit les développeurs et les organisations réutiliser massivement des composants de code prêts à l'emploi voir des programmes entiers, qui pourraient être infectés par de telles portes dérobées. Mais contrairement aux vulnérabilités logicielles traditionnelles, les portes dérobées constituent actuellement une menace presque totalement non mitigée. Il existe en effet un grave manque de données sur la variété des portes dérobées répandues dans la nature, tandis que les rares méthodes de détection existantes souffrent d'une portée, d'une automatisation et d'une applicabilité restreintes.
Dans ce projet, nous visons à construire les premiers moyens systématiques d'atténuer la menace posée par les portes dérobées logicielles. Tout d'abord, nous introduisons un modèle générique de portes dérobées et proposons de l'évaluer et de l'affiner par rapport à un large ensemble d'échantillons de portes dérobées que nous allons systématiquement récolter. Deuxièmement, nous concevons une méthode de détection des portes dérobées qui respectent ce modèle, conçue pour être aussi automatisée et adaptable que possible, et nous l'évaluons par rapport à une variété de portes dérobées existantes.

*Intervenant