Procédures de décision pour l'analyse de vulnérabilités

Benjamin Farinier*[1]

[1]CEA LIST (CEA-LIST) – Commissariat à l'énergie atomique et aux énergies alternatives – CEA LIST, LSL, Université Paris-Saclay, Gif-sur-Yvette, France

Résumé

L'Exécution symbolique est une technique de vérification formelle qui consiste en modéliser les exécutions d'un programme par des formules logiques pour montrer que ces exécutions vérifient une propriété donnée. Très efficace pour la recherche de bogues, il est question aujourd'hui de l'employer dans d'autres contextes, comme en analyse de vulnérabilités. L'application de l'Exécution symbolique à l'analyse de vulnérabilités diffère de la recherche de bogues sur au moins deux aspects:

- Les formules logiques générées au cours de l'Exécution symbolique deviennent rapidement gigantesques et de plus en plus difficiles à résoudre pour les solveurs.

- La modélisation de certaines propriétés de sécurité est susceptible de faire intervenir des quantificateurs dont l'emploi rend les formules logiques générées presque impossibles à résoudre.

Cette thèse porte donc sur ces deux problématiques issues du domaine des procédures de décision, visant à permettre des modélisations plus fines nécessaires à l'analyse de vulnérabilités.

*Intervenant