Génération d'exploits utilisant des techniques de preuve formelle

Guillaume Cluzel*[1]

[1]TrustInSoft – TrustInSoft – France

Résumé

La majorité des couches bas-niveau des systèmes informatiques sont écrites en C. Une large classe de comportements non définis par la norme du C laissent la place à des attaques logicielles aux conséquences souvent lourdes. L'utilisation de l'analyse statique, notamment grâce à l'interprétation abstraite, permet de supprimer la totalité de ces défauts logiciels. Mais la défaillance d'un programme peut aussi provenir d'une mauvaise implémentation d'un protocole donné. Dans ce cas, l'écriture de spécifications ainsi que leur preuve automatique est une piste privilégiée pour garantir la sécurité du logiciel.

*Intervenant