

---

# Etude de propriétés d'opacité temporisée à l'aide de vérification temporisée paramétrée

Dylan Marinho\*<sup>1</sup>

<sup>1</sup>Laboratoire Lorrain de Recherche en Informatique et ses Applications – Institut National de Recherche en Informatique et en Automatique, Université de Lorraine, Centre National de la Recherche Scientifique : UMR7503 – France

## Résumé

Une fuite d'informations peut avoir des conséquences dramatiques sur la sécurité d'un système. Parmi ces failles, une fuite d'informations temporelle se produit lorsqu'un attaquant peut déduire des informations internes confidentielles en basant son attaque sur une observation temporisée du système. Nous modélisons ici le système par un automate temporisé, et considérons qu'un attaquant a accès (uniquement) au temps d'exécution du système. Nous abordons deux problèmes d'opacité temporisée : déterminer les temps d'exécution pour lesquels le système est sécurisé (c'est-à-dire pour lesquels l'attaquant ne peut pas déduire d'information confidentielle) et déterminer si un système est sécurisé pour tous ses temps d'exécution possibles.

---

\*Intervenant