Guaranteeing Timed Opacity using Parametric Timed Model Checking

Dylan Marinho*[1], Etienne André[2], Didier Lime[3], and Sun Jun[4]

[1]Université de Lorraine, LORIA – Université de Lorraine, CNRS, LORIA, F-57000 Metz – France
[2]Université de Lorraine, CNRS, Inria, LORIA, Nancy, France – Université de Lorraine – France
[3]LS2N – Nantes Université - École Centrale de Nantes, CNRS : UMR6004 – France
[4]School of Information Systems, Singapore Management University, Singapore – Singapour

Résumé

Information leakage can have dramatic consequences on systems security. Among harmful information leaks, the timing information leakage occurs whenever an attacker successfully deduces confidential internal information depending on the system execution time. We address the following timed opacity problem: given a timed system, a private location and a final location, synthesize the execution times from the initial location to the final location for which one cannot deduce whether the system went through the private location. We also consider the full timed opacity problem, asking whether the system is opaque for all execution times. We show that these problems are decidable for timed automata (TAs) but become undecidable when one adds parameters, yielding parametric timed automata (PTAs). We then devise an algorithm for synthesizing PTAs parameter valuations guaranteeing that the resulting TA is opaque and finally show that our method can also apply to program analysis.

*Intervenant