Guaranteeing Timed Opacity using Parametric Timed Model Checking

Étienne André, Didier Lime, Dylan Marinho and Sun Jun

Dylan.Marinho@loria.fr

1 Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
2 École Centrale de Nantes, LS2N, UMR CNRS 6004, Nantes, France
3 School of Information Systems, Singapore Management University, Singapore

Context: timing attacks

- Principle: deduce private information from timing data (execution time)
- Issues:
  - May depend on the implementation (introduced by the compiler)
  - A relatively trivial solution: make the program last always its maximum execution time

Drawback: loss of efficiency

Informal problems

- Question: can we exhibit secure execution times?
- Further question: can we also tune internal timing constants to make the system resisting to timing attacks?

Objective. Given a system modeled by a timed automaton, can we exhibit secure execution times, i.e., for which an attacker having only access to the global execution time cannot deduce whether some private location was visited?

Formalism: Timed Automaton (TA) [AD94]

A timed automaton (TA) is a 7-tuple: 

\[
\text{T} = \langle \text{locations}, \text{actions}, \text{clocks}, \text{clock init}, \text{clock reset}, \text{clock guard}, \text{tm} \rangle
\]

- \text{locations} are sets of locations and actions
- \text{clocks} are sets of clocks
- \text{clock init} are sets of clock initial values
- \text{clock reset} are sets of clock reset functions
- \text{clock guard} are sets of clock guard functions
- \text{tm} is a transition relation

Experiments [TOSEM22]

Perspectives

Results

- Answer the timed opacity problems (TA), exhibiting which execution times are opaque, and whether all execution times indeed guarantee opacity
- Answer the synthesis problem (PTA) exhibiting at least some valuations for which the system can be made opaque

Overview of our theoretical results [TOSEM22]

- General case: The mere existence of a parameter valuation for which there exists a duration for which timed-opacity is achieved is undecidable
- Study of a subclass known for being “at the frontier” of decidability (L/U-PTA) [Hun+02]
- Practical contribution: We adopt a “best-effort” approach for the general case of PTAs: this approach is not guaranteed to terminate

In summary, the main contributions of this work are:

- A new method for checking timed opacity
- A tool for automatically synthesizing parameter valuations
- A benchmark library for comparing different approaches

References


This work was partially supported by the ANR-DFR Fronck-Singapour research program PhdFit (ANR-18-CES-0015).