Development and Industrial Application of Multi-Domain Security Testing Technologies

Innovation Sheet
Passive Symbolic Monitoring
Passive Testing Using Symbolic Approach

Description

- Passive testing = Based on the **control + data portions** of the messages to avoid false positive verdicts.

- Symbolic Passive testing integrates two important techniques:
  - **Symbolic Execution of the Input-Output Symbolic Transition System (IOSTS)**: The property and/or attack sequence to be monitored are modelled using IOSTS.
  - **Parametric Trace Slicing**: Real-time trace analysis.

- Traces are obtained using Wireshark or any Trace analyser.

- The trace obtained is sliced based on certain parameters of interest according to our **slicing logic**. For the different parametric instances observed in the trace, different slices are obtained.

- Each slice is verified (control + data portions) against the property/attack sequence passively by pattern matching and substitution (symbolic values by concrete values, if the guard-conditions are satisfied) logics.

- A verdict Pass/Fail/Attack-Pass/Attack-fail/Inconclusive is obtained based on the **evaluation logic** implemented in our prototype model.
Passive Testing using Symbolic approach
State of the art

- Passive testing using invariants: several approaches are published
  - ‘Formal passive testing of timed systems: theory and tools’
  - ‘Timed extended invariants for the passive testing of web services’
  - ‘A formal data-centric approach for passive testing of communication protocols’

- Passive Testing using EFSM:
  - ‘An EFSM-based passive fault detection approach’

- Active Testing using Symbolic execution techniques
  - ‘Symbolic execution techniques for test purpose definition’
  - ‘Integrating formal verification and conformance testing for reactive systems’
Passive Testing Using Symbolic Approach
Advances beyond the state of the art

- From our knowledge, there are currently no works tackling Passive testing/Monitoring based on IOSTS without any awareness on the states of the execution traces, moreover:
  - the integration of symbolic execution of IOSTS and Slicing technique for Passive Testing was a completely new idea.
  - dealing with symbolic values eliminates the necessity of enumeration of all data values.
  - the approach enables testing functional and vulnerability/attack patterns by passive testing.

[Deliverable D4.WP1, Section 6.6]
Passive Testing Using Symbolic Approach
Application to case studies

- Symbolic Passive Testing was applied to Automotive case study (DCo).
- A prototype of a Symbolic passive testing tool was developed.
- In the future: to be applied on runtime traces for online monitoring.