DIAMONDS

Development and Industrial Application of Multi-Domain Security Testing Technologies

Innovation Sheet
Passive Symbolic Monitoring

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

© DIAMONDS Consortium 2010-2013

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 '
- C. Andres, M. G. Merayo, M. Nunez, Software: Testing, Verication and Reliability 22 (2012) 365-405
  - 'Timed extended invariants for the passive testing of web services'
- G. Morales, S. Maag, A. Cavalli, W. Mallouli, E. de Oca, in: Proceedings of the 8th IEEE ICWS, 2010, pp. 592-599.
  - 'A formal data-centric approach for passive testing of communication protocols'
- F. Lalanne, S. Maag, IEEE/ACM Transactions on Networking PP (99).

- Passive Testing using EFSM:
  - 'An EFSM-based passive fault detection approach'
- H. Ural, Z. Xu, An EFSM-based passive fault detection approach, in: Testing of Software and Communicating Systems, 19th IFIP, 2007, pp.335-350

- Active Testing using Symbolic execution techniques
  - 'Symbolic execution techniques for test purpose definition'
- C. Gaston, P. L. Gall, N. Rapin, A. Touil, in: 18th IFIP Testing of Communicating Systems (TestCom), 2006, pp. 1-18
  - 'Integrating formal verification and conformance testing for reactive systems'
- C. Constant, T. Jeron, H. Marchand, V. Rusu, IEEE Trans. Software Eng. 33 (8) (2007) 558-574.

© DIAMONDS Consortium 2010-2013

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]

© DIAMONDS Consortium 2010-2013

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.

© DIAMONDS Consortium 2010-2013