Development and Industrial Application of Multi-Domain Security Testing Technologies

Innovation Sheet
Integration of Model Based Test Generation and Monitoring

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Integration of MBT and Monitoring
Description

- **Two complementary techniques**
  - Model based generation of abstract test cases, their concretization and execution against the SUT
  - The analysis of the SUT responses in order to assign the test verdict and automate the detection of vulnerabilities.
- **More details**
  - The Modeling activity aims to define a model that captures the behavioral aspects of the SUT in order to generate consistent (from a functional point of view) sequences of stimuli
  - The Test Purposes activity consists in formalizing test purposes from vulnerability/ attacks test patterns that the generated test cases have to cover
  - The Test Generation and Adaptation activity consists in automatically producing abstract test cases from the artefacts defined during the two previous activities
  - The Concretization and test Execution activity aims to translate the generated abstract test cases into executable scripts and to execute them on the SUT.
  - The monitoring activity consists in analyzing the communication with the SUT and checking a set of properties to assign the test verdict

Integration of MBT and Monitoring
State of the art

- Usually seen as two different techniques
  - Active testing: testing phase – conformance testing is already a standard

    ISO 9646. Information Technology, Open Systems Interconnection, "Conformance Testing Methodology and Framework". International Standard IS-9646. ISO, 1991. CCITT X.290–X.294
  - Passive testing: operation phase

    David Lee, Arun N. Netravali, Krishan K. Sabnani, Binay Sugla, Ajita John: "Passive testing and applications to network management". ICNP 1997
  - Several tools have been specified and implemented in the research field

    http://en.wikipedia.org/wiki/Test_automation

    Ana R. Cavalli, Edgardo Montes de Oca, Wissam Mallouli, Mounir Lallali: Two Complementary Tools for the Formal Testing of Distributed Systems with Time Constraints. DS-RT 2008:315-318
- Integration of active and passive testing rarely elaborated
  - Application of active and passive testing to telecommunication protocols (functional testing)

    Yixin Zhao, Jianping Wu, Xia Yin: From Active to Passive - Progress in Testing Internet Routing Protocols. J. Comput. Sci. Technol. (JCST) 17(3):264-283 (2002)
  - Application of active and passive testing to security

    Guoqiang Shu, David Lee: Message Confidentiality Testing of Security Protocols - Passive Monitoring and Active Checking. TestCom 2006:357-372

Integration of MBT and Monitoring
Advances beyond the state of the art

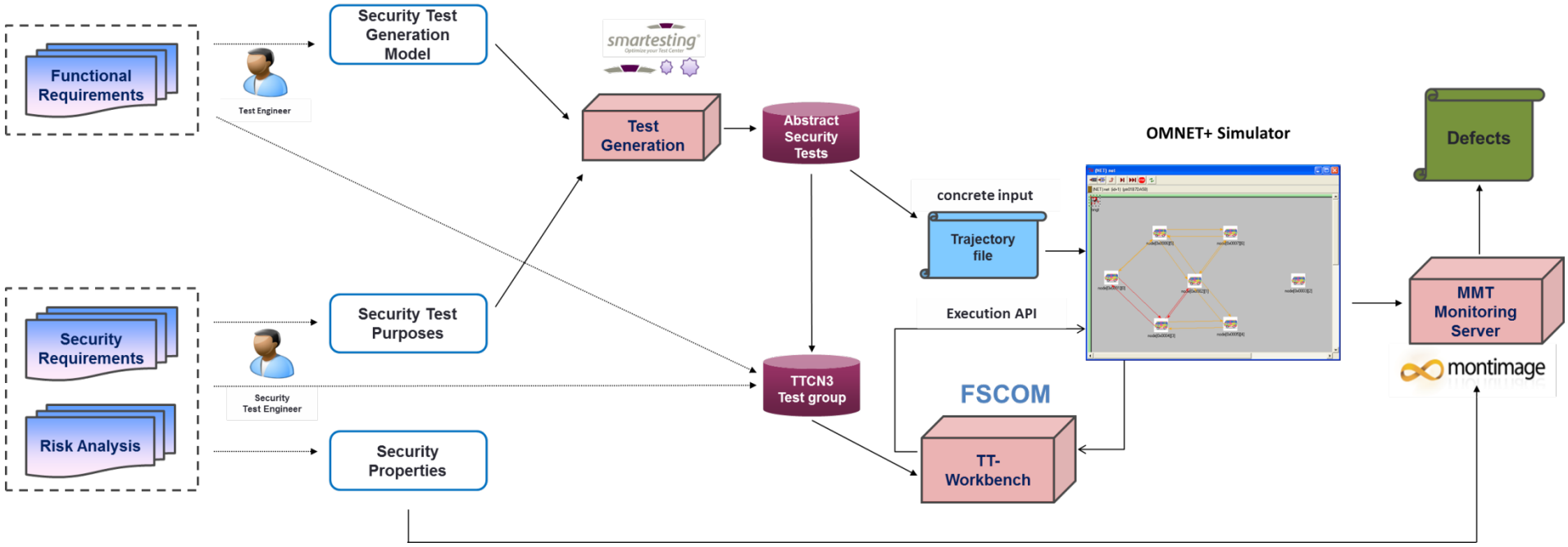
- During the modeling activity, the observations (desired behavior) are not specified or partially specified within the functional model.
  ⇒Less effort (time and money) to build the behavioral model
  ⇒The stimuli generation can be random or based on intelligent fuzzing
  [Deliverable D2.WP2, section 2.2]

- The test purposes that guide the test cases generation are not specifically related to the security properties that we want to check on the collected traces (data sources can be distributed).
  [Deliverable D2.WP2, Section 1.4]
  [Deliverable D3.WP2, Section 1.1]

- The technique is very interesting when the tester has a partial knowledge of the impact of its stimuli on the SUT. An attack can violate more that one security property.
  [Deliverable D4.WP1, Section 5]

Integration of MBT and Monitoring
Exploitation and application to case studies

- Thales radio protocols case study



Integration of MBT and Monitoring
Exploitation and application to case studies

- Gemalto TSM case study