Development and Industrial Application of Multi-Domain Security Testing Technologies

Case Study Experience Sheet
Radio protocol Study from Thales Communications & Security

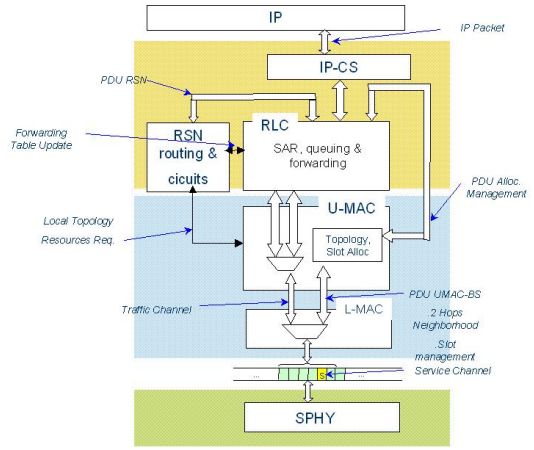
ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

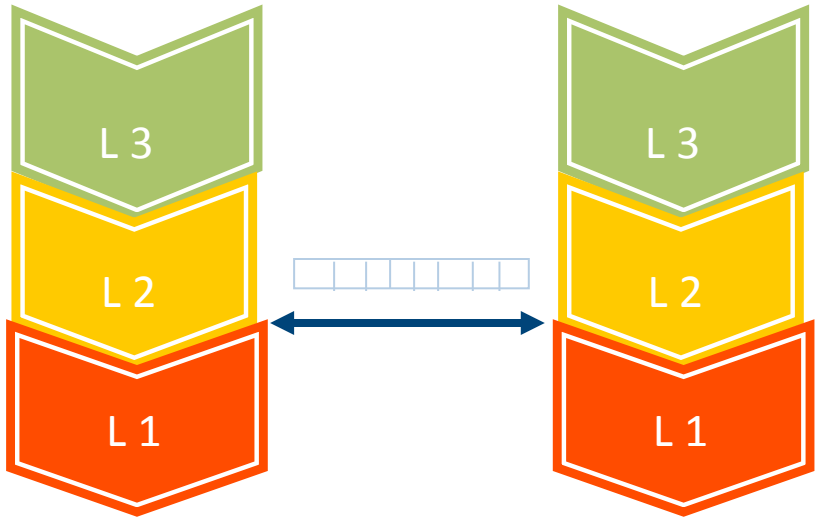
Radio Protocol Case Thales

Case study characterization

Layered protocol stack

- Automatic network : no initial planning
- Network continuity whatever are the stations in the network
- “on the move” automatic network re-organization and operation
- End-to-end heterogeneous user services transmission : voice, messages
- Decentralized mesh network. no BS
- Vulnerability analysis based on the OTA frames exchanges
- Experiments on the exchanges between the L1/L2 layers PDU frames

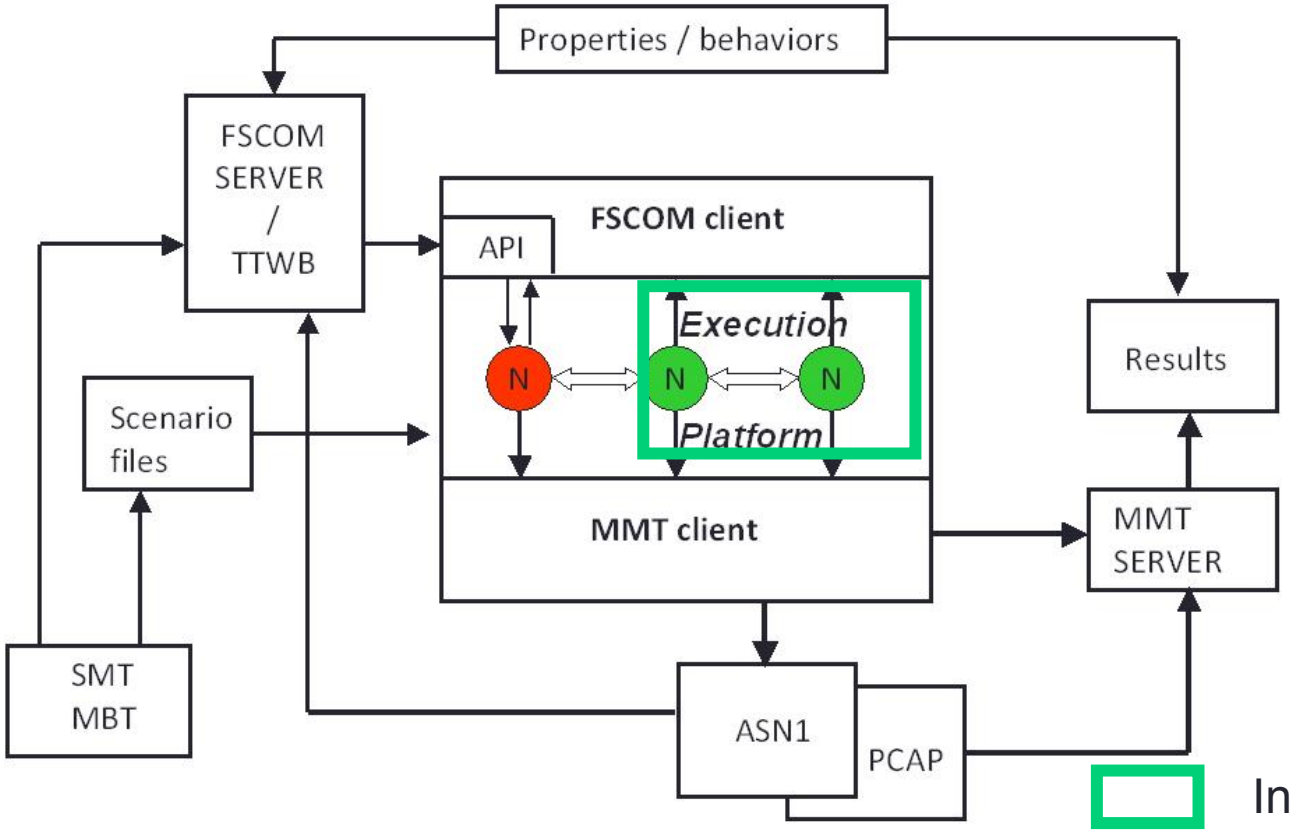




ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Radio Protocol Case Thales

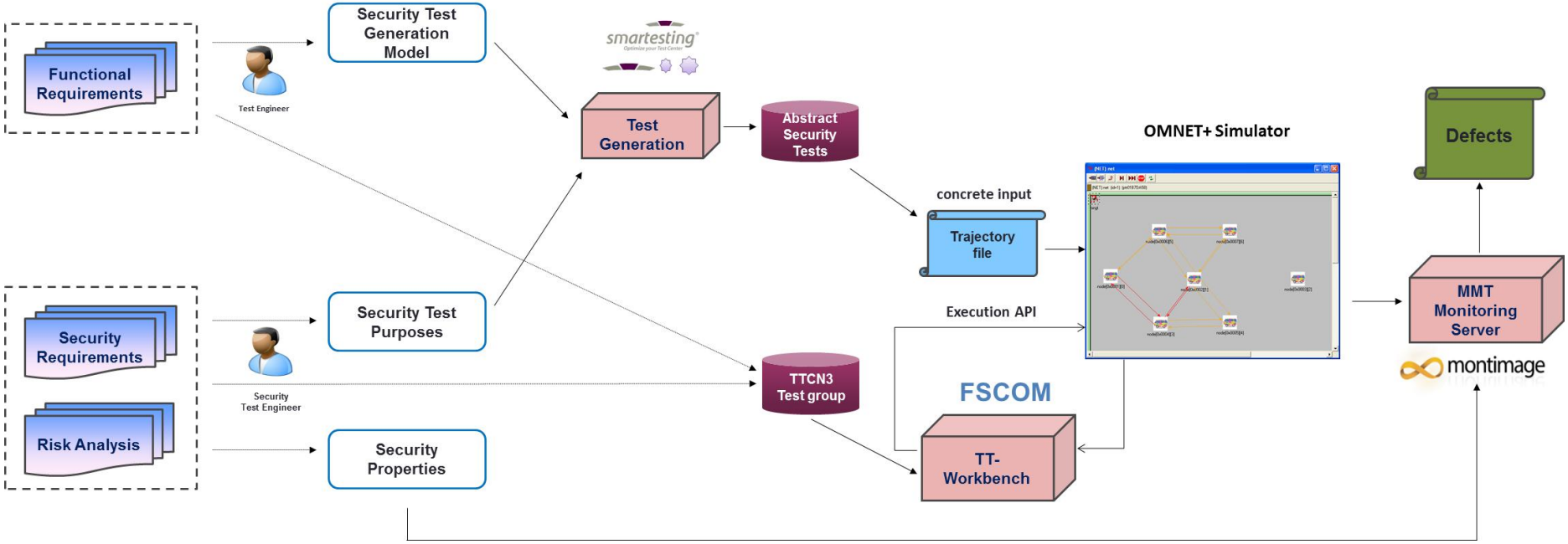
Case study characterization



- Security challenges
  - **Offline & online /Passive & active testing**

Radio Protocol Case Thales

Testing approach: active testing & montoring



- ***SMARTESTING***
  - Security test generation model and test purposes specification
  - Generation of test scenarios denoting attacks using Certify-it
- ***FSCOM***
  - TTCN3 test cases specification
  - Test execution using TT-Workbench

- ***MONTIMAGE***
  - Specification of 19 security properties
  - Client /Server architecture
  - Notification of exchanged PDUs
  - Parsing and extraction of relevant information
  - Online analysis of captured PDUs and detection of attacks occurrences

Radio Protocol Case Thales
Results

- **Integration of the tools in the TCS validation framework, use of standardized API to help on the integration on different validation environment and industrial domains.**
- **Validation of the framework with the validation of 19 security properties. Implementation of 7 intrusion attacks.**
- **Further work with IT :distributed detection of several attackers at routing layer and LIG: genetic testing for static analysis of memory overflow.**

Radio Protocol Case Thales
Exploitation

- **DIAMONDS satisfies the requirements of higher security testing, in particulat on Over The Air threats.**
- Evolution of security testing from the critical components to the whole parts of the radio equipment (Hw platform, midleware and radio protocol application).
- DIAMONDS is a first response the security testing analysis of these applications for which tools and methodologies are lacking.
- Next step might be the integration of Intrusion Detection & Prevention System in the radio equipments.

Radio Protocol Case Thales
Summary

- **Improvement gains according to DIAMONDS STIP:**