Development and Industrial Application of Multi-Domain Security Testing Technologies

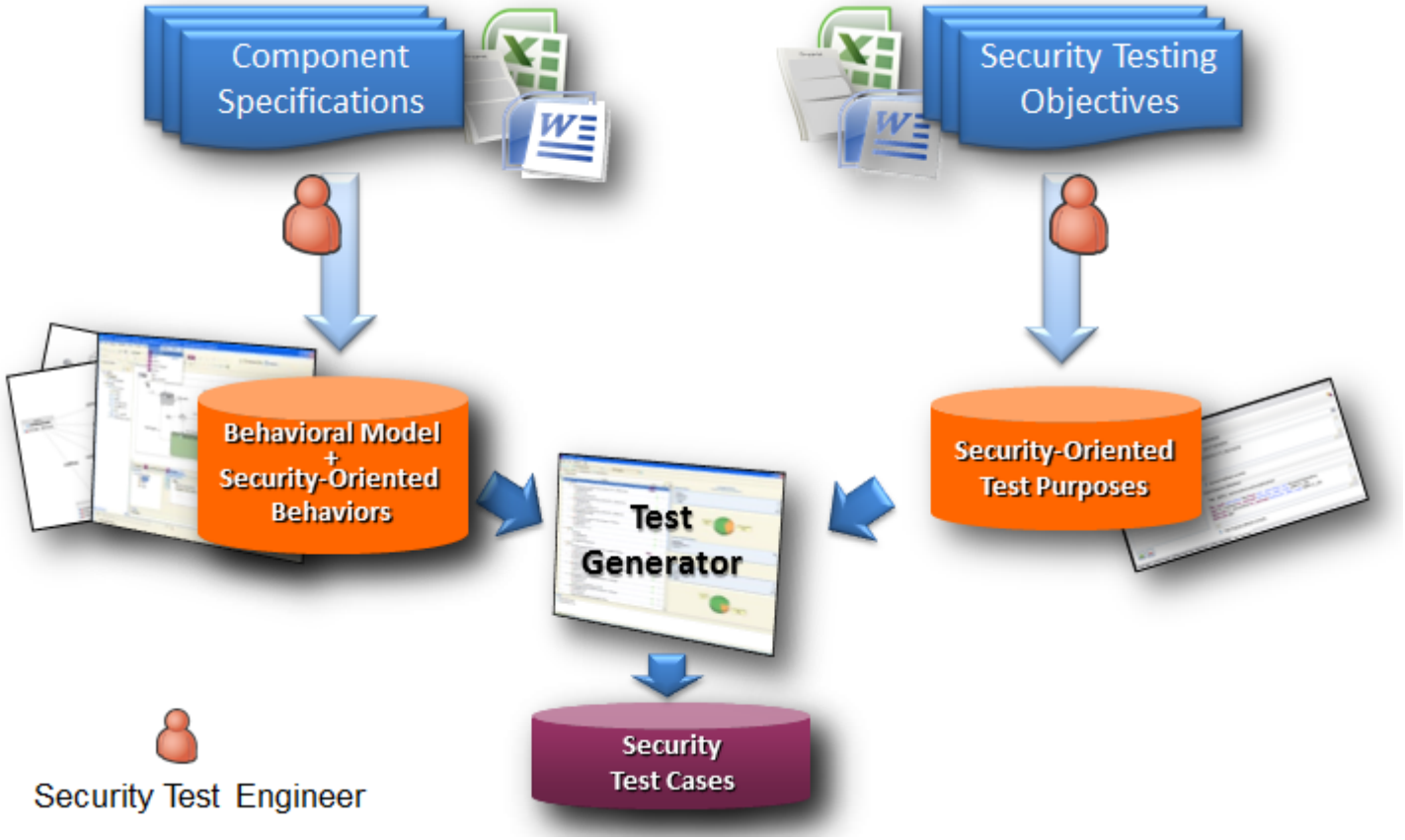
Innovation Sheet

Model-Based Security Testing from Behavioural Model and Test Purposes

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Security Testing from Models and Test Purposes
Description

Test generation for security properties and logical vulnerabilties



Security Testing from Models and Test Purposes
Description

Motivation

- Accurate and precise automated test generation of security test
- Test generation for security properties and logical vulnerabilities (vulnerabilities related to the behavior fo the system under test).

Process

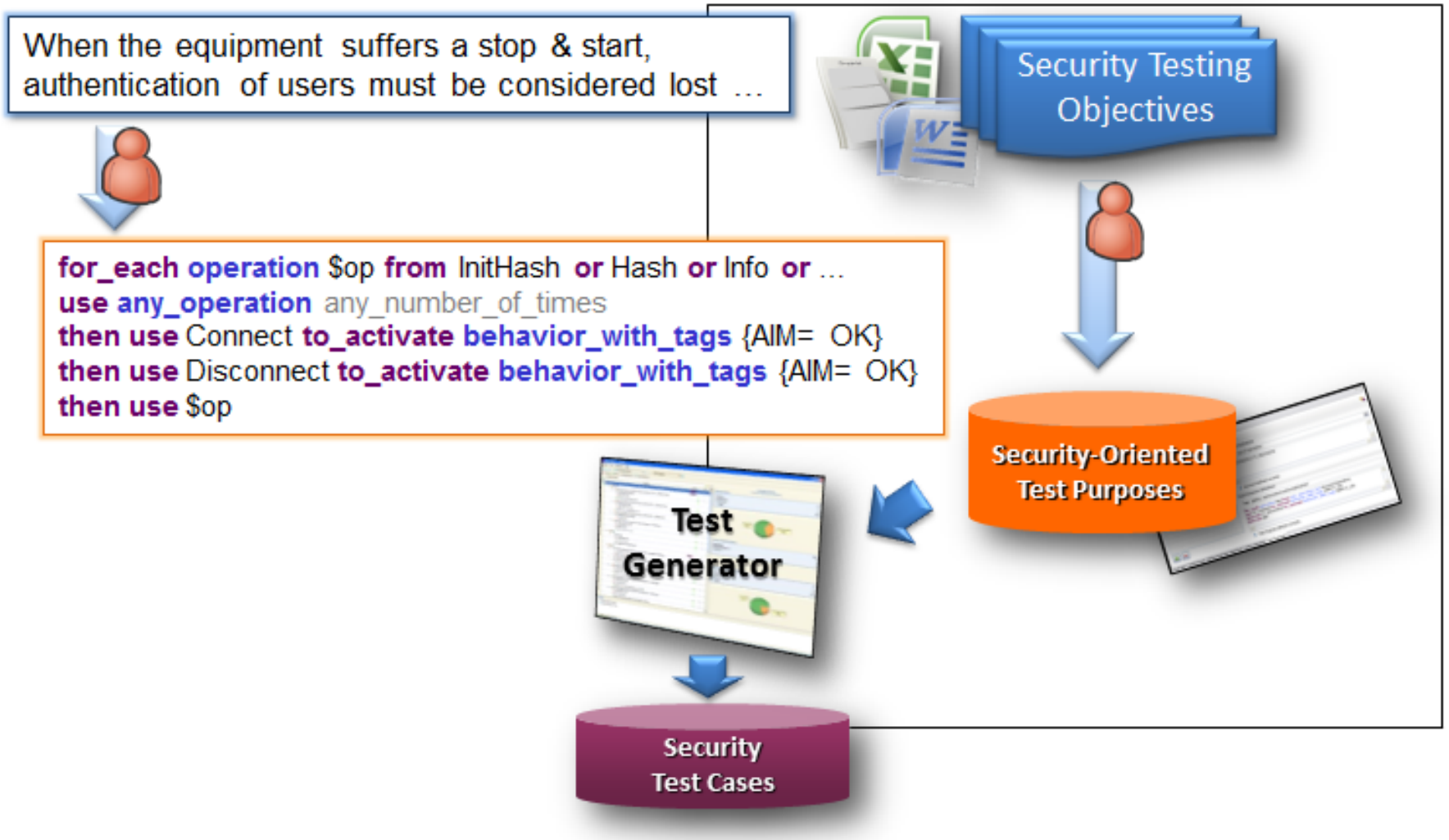
- Test purposes come first: they formalize the security test patterns
- The modeling elements are limited to behavioral / environemental aspects of the system under test to be composed with the test purpose

Innovation

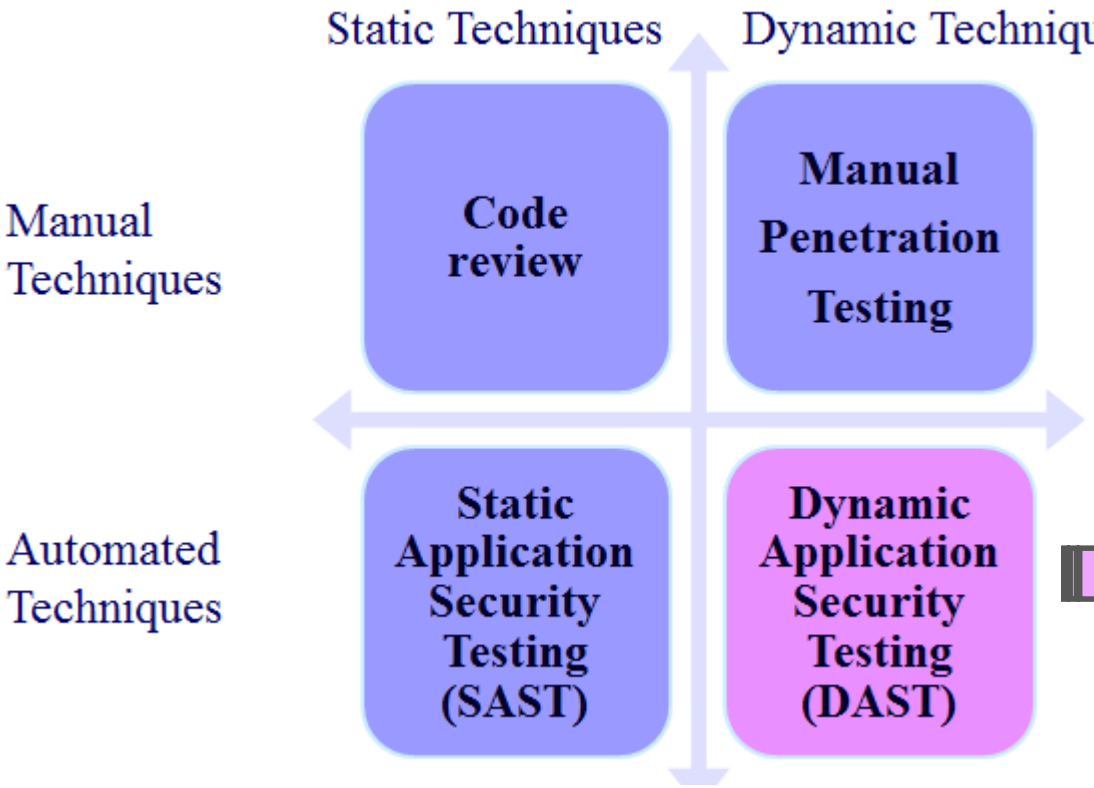
- The test purpose language is original and fully designed to support the formalisation of Security Test Patterns
- The test generation engine has been adapted to efficiently compose behavioral/ environmental model with test purposes

Security Testing from Models and Test Purposes
Description

Example of test purpose formalized from a security requirement



Security Testing from Models and Test Purposes
State of the art



Security test engineers and petetration testers are using mainly **three DAST tool categories**:

- Web application vulnerability scanners
- fuzzing tools
- intrusive proxies

Model-based security testing from behavioral model and test purpose allows better accuracy and precision in security property testing and logical vulnerability detection

Security Testing from Models and Test Purposes

Advances beyond the state of the art

- Improvements of the accuracy and precision of security property testing and logical vulnerability testing by means of models and test patterns, still keeping a high level of automation.
  - Accuracy - The capability to focus vulnerability testing on the relevant part of the software (e.g. from a risk assessment point of view) depending on the targeted vulnerability types.
  - Precision - The capability to avoid both false positive and false negative.

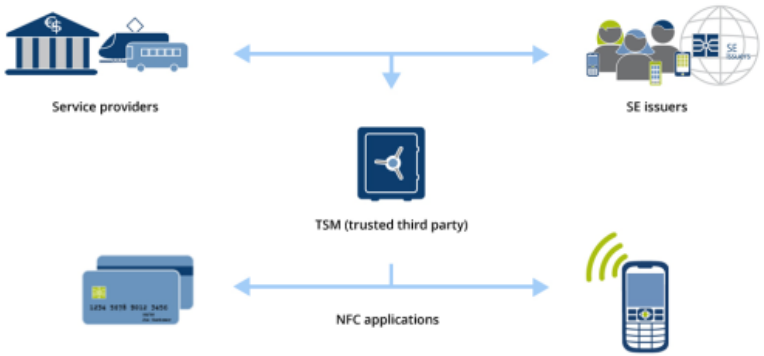
[Deliverable D5.WP2, section C.II]

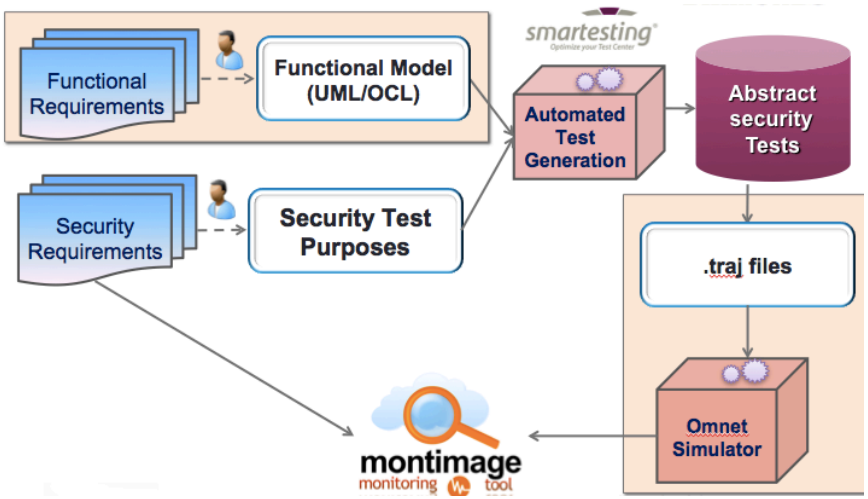
- Capitalization on generic test patterns and generic modeling aspects that may be used on a specific domain (such as web applications, security components, ….)

[Deliverable D3.WP3, section 7]
[Deliverable D5.WP3, section 2.5]

Security Testing from Models and Test Purposes
Application to case studies

Gemalto Trusted Service Manager





THALES Software Radio

SINTEF / NORSE Banking application – vulnerability test generation for SQL Injection

Itrust application: first experiments of model definition and test execution

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT