3rd UCAAT User Conference on Advanced Automated Testing

ETSI World Class Standards

Sophia Antipolis, French Riviera
20-22 October 2015

EXPERIENCE REPORT ON MODEL-BASED TESTING OF SECURITY COMPONENTS

Presented by Elizabeta Fourneret

femto-st sciences & technologies

3rd UCAAT User Conference on Advanced Automated Testing

ETSI World Class Standards

EXPERIENCE REPORT ON MODEL-BASED TESTING OF SECURITY COMPONENTS

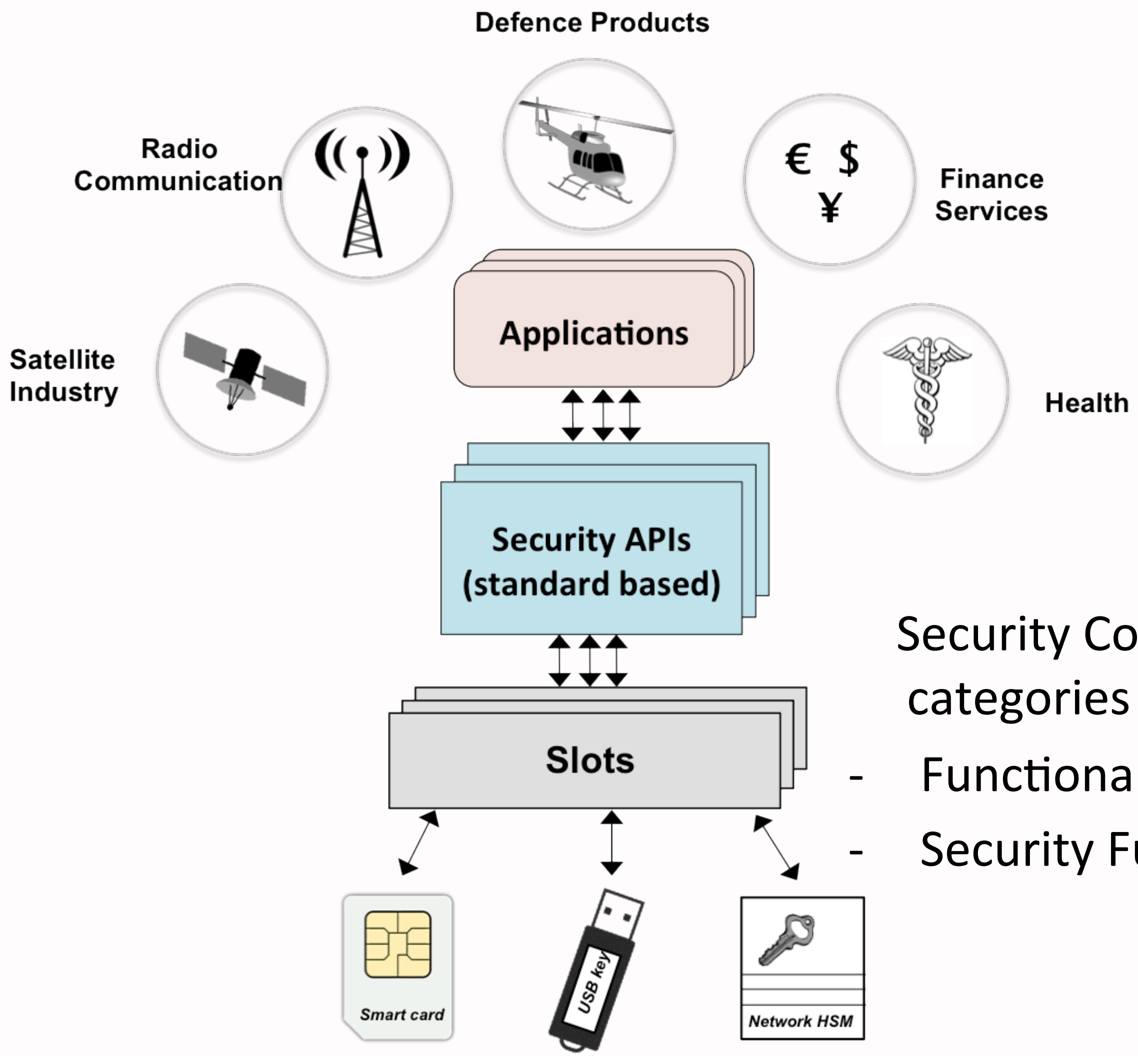
Frédéric Dadeau, Elizabeta Fourneret

femto-st sciences & technologies

Outline

- Introduction
- Our MBT approach
- Experimental results
- Conclusion and perspectives

Security Components

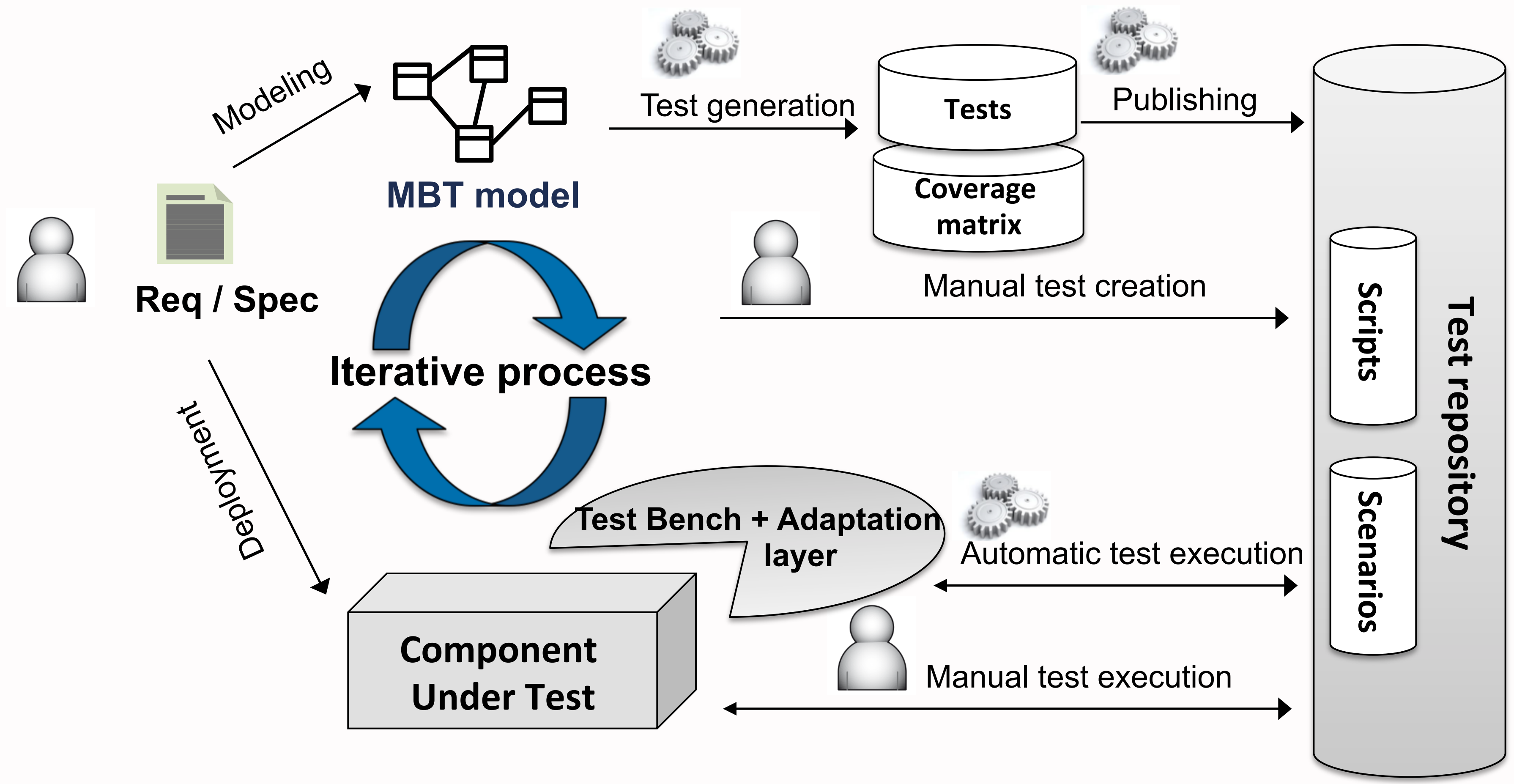


Security Components have two categories of test requirements:

- Functional Requirements
- Security Functional Requirements

20-22/10/2015

Model-Based Testing



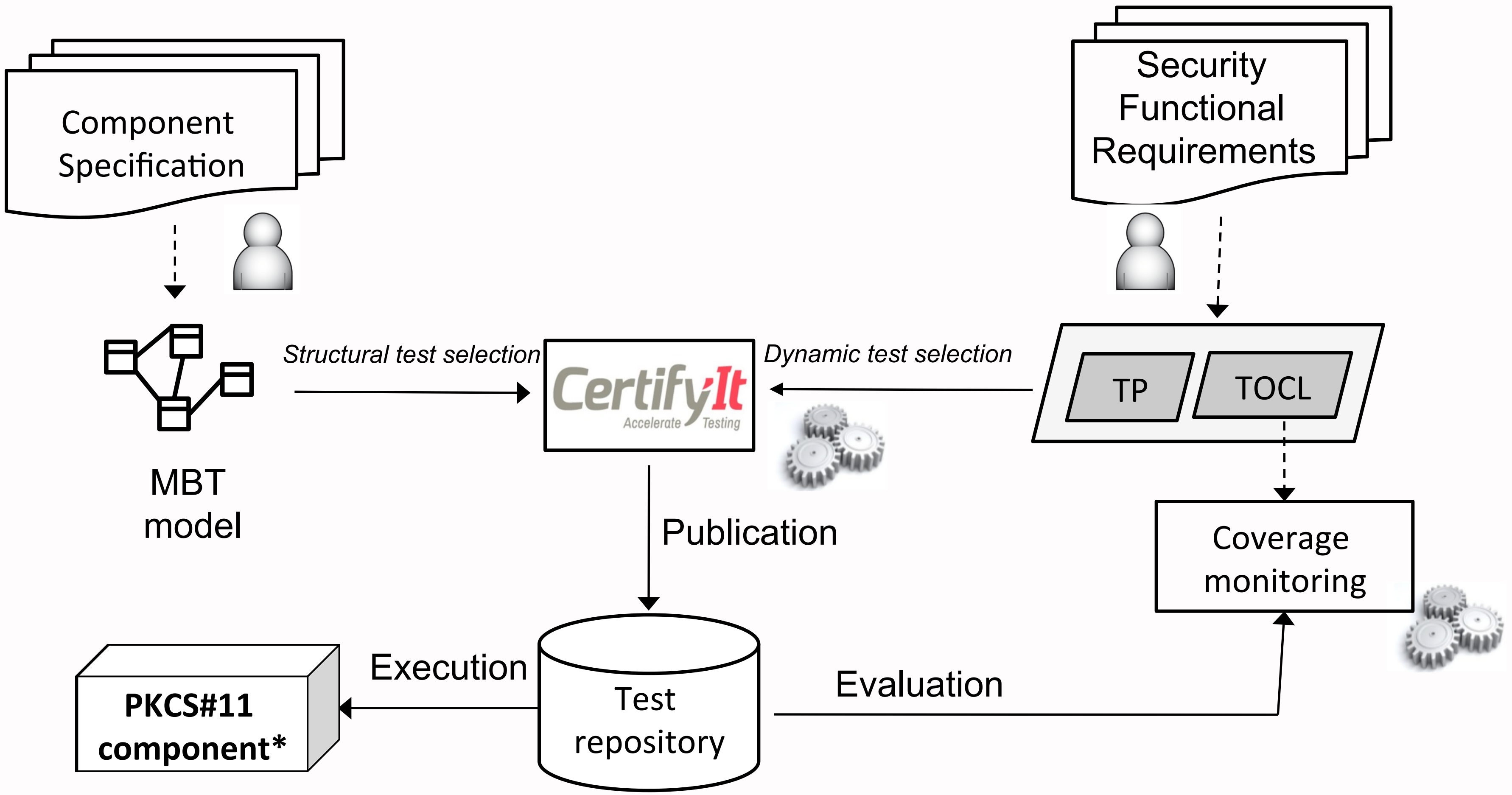
Motivation

- Limitations of automated testing based on structural (for ex. requirement) coverage
  - test cases with limited size (steps)
  - difficulty to take into account the dynamics of the security functional requirements (must be hard-coded into the model)
  - possible issues with the test target's reachability
- Our proposal: use temporal properties in TOCL and Test Purposes
  - How to express the test requirements easily?
  - How to characterize relevant tests?

Outline

- Introduction
- Our MBT approach
- Experimental results
- Conclusion and perspectives

Our MBT Approach



*SoftHSM Virtual Cryptographic Token created by the group OPENDNSSEC

TOCL and TP test selection criteria

- **TOCL** and **TP** make possible to generate tests that exercise **corner cases**, relevant when testing security components
- **TOCL** allows to express **temporal properties**, for instance of succession or precedence, contributing to the MBT process with:
  - Evaluation of the existing tests coverage
  - Verification of the model's conformance to these properties
    - ➢ Simplifying the model debugging
- **TP** allow to express **procedures of tests** based on a verbose representation and using the experts experience and knowledge

Outline

- Introduction
- Our MBT approach
- Experimental results
- Conclusion and perspectives

PKCS#11 and SoftHSM

- PKCS#11 is an RSA standard that defines an interface called Cryptoki to promote interoperability and security of cryptographic tokens.
- Scope: 24 functions most commonly present in the tokens, such as session, token, key and user management functions, as well as cryptographic functions for signing messages and verifying signatures.
- To ensure the repeatability of the MBT process we chose SoftHSM - virtual cryptographic store largely used for exploring PKCS#11 without the necessity to posses an HSM (created by the group OPENDNSSEC).

Experimental results

Case study: PKCS#11

Component Under Test: SoftHSM

1st experiment: evaluation of complementarity of test selection criteria to cover test requirements

2nd experiment: evaluation of the error detection capabilities (robustness)

*funded by the French National Research Agency

Experimental results

PKCS#11 set up metrics

Test Requirement category	#FR	#SFR
general purpose	7	4
slot and token management	22	5
session management	32	9
object management	6	1
digesting	28	9
signing	32	10
verifying signatures	31	10
total	158	48

PKCS#11 model element	
#classes	9
#enumerations	20
#enum. literals	123
#associations	17
#class attributes	34
#operations	24
#observations	1
#behaviors	206
#tocl properties	50
#test purposes	5
#LOC	1308

LOC: Lines of OCL constraints

Experimental results

PKCS#11 results metrics

Test Selection Criterion	#Test targets	#Test cases	Cov. in % FR	Cov. in % SFR
Structural	206	184	100	40
TOCL	311	90	31	58
Test Purpose	24	24	9	2
Manual	24	24	45	/

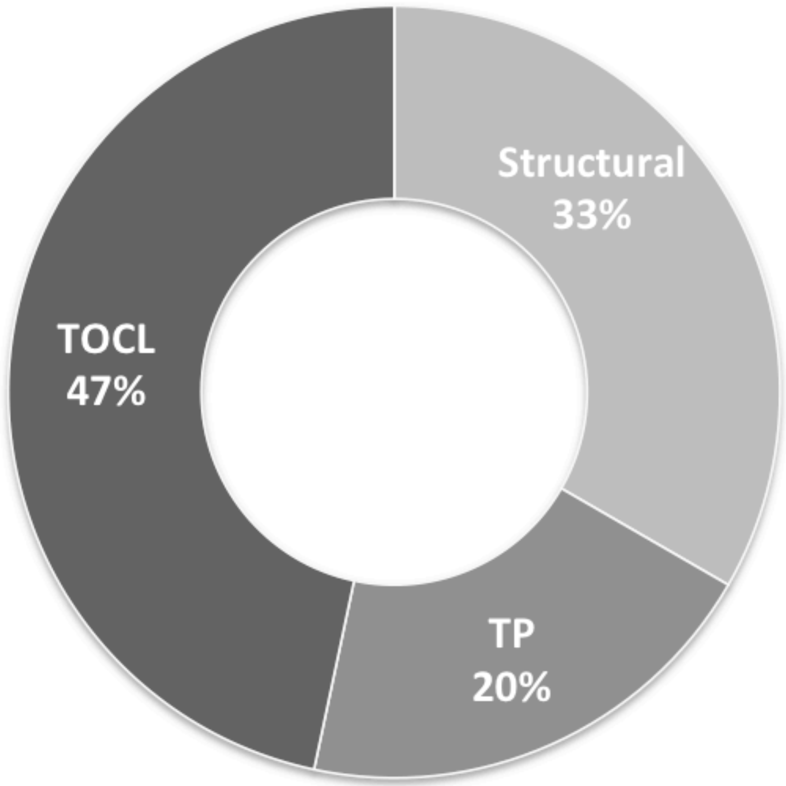


Fig. Distinct fault detection capabilities per coverage requirement

Cost of applying the approach
~ 20 person / days

Experimental results

Conclusions of the study:

- Relevance of the TOCL and TP coverage criteria
  - "Produce tests that one may not easily think of"
  - augment test requirements coverage
- TOCL and TP increase fault detection capabilities
- Usefulness of coverage reports
  - show which part of the requirements are not covered by the tests
- Cost-benefices:
  - cost of applying TOCL and TP coverage criteria is very low
  - cost for regression testing (for ex. At the end of a sprint) is negligible
- Use of the TOCL properties: model validation
  - Use of the TOCL coverage measure to detect violations of the properties by the model

Outline

- Introduction
- Our MBT approach
- Experimental results
- Conclusion and perspectives

Conclusion

- We have experienced an MBT approach :
  - Combining static and dynamic test selection criteria
  - On a real-life security components

- Useful for:
  - Evaluating a test suite w.r.t. security requirement
  - Test selection, to augment a functional test suite
  - Increasing distinct fault-detection

Perspectives

- Test generation process
  - Online (fuzz) testing
  - Robustness criteria (based on TOCL automata coverage)

- **Looking forward for other pilot projects to foreground our results.**

Thanks for your attention!

Questions?