ETSI

World Class Standards

SECURITY IN MTS
26 APRIL 2013
SIG OVERVIEW

Fraunhofer FOKUS

ETSI TC MTS

TC Methods for Testing and Specification

- Overview of MTS working fields
  - **Specification** techniques
    - Test requirements, purposes
  - **Testing** languages
    - TTCN-3, TPLan, TDL
  - **Model-based testing approaches**
  - Testing methods: conformance, interoperability, performance, **security**, …

MTS Security work items

With input from European research projects:

(1) Terminology, Concepts, Lifecycle

Overview on used terminology (w/o redefining)

(2) Case studies

Security testing experiences from research (e.g. *DIAMONDS*: model-based, fuzzing)

(3) Design guide V&V

Guidance to the system designers enabling validation and verification

(1) Terms and concept details

- **security testing** = static analysis (w/o execution) + **dynamic analysis** (execute)
- **security testing types**: features/functionality, performance/load/stress, robustness/reliability
- **security testing tools**: vulnerability scanner, port scanner, fuzzing tools, monitoring/instrumentaion
- **security testing verdicts** = pass/fail/inconc

(1) Terms and concept details (cont.)

- **Security testing requirements**:
  Analysis of Hazard/Threat, Vulnerability, Risks
- **Functional security testing**
  refers to ISO 9646 (CTMF) and ISO 15408 (CC)
- **Performance testing for security**
  demonstrate what happens when limits are reached
- **Fuzzing testing**
  - Smart Fuzzing: behavioural model of interface
  - Dumb Fuzzing: structural model of communication from network activity capture/files)

(1) „Terminology“ (stable draft)

3 Definitions, symbols and abbreviations

4 Introduction to security testing

- 4.1 Types of security testing
- 4.2 Testing tools
- 4.3 Test verdicts in security testing

5 Use cases for security testing

6 Security test requirements

- 6.1 Risk-assessment and analysis

7 Functional security test

8 Performance testing for security

9 Fuzz testing

- 9.1 Types of fuzzers
- 9.2 Fuzzing test setup and test process
- 9.3 Fuzzing requirements and metrics

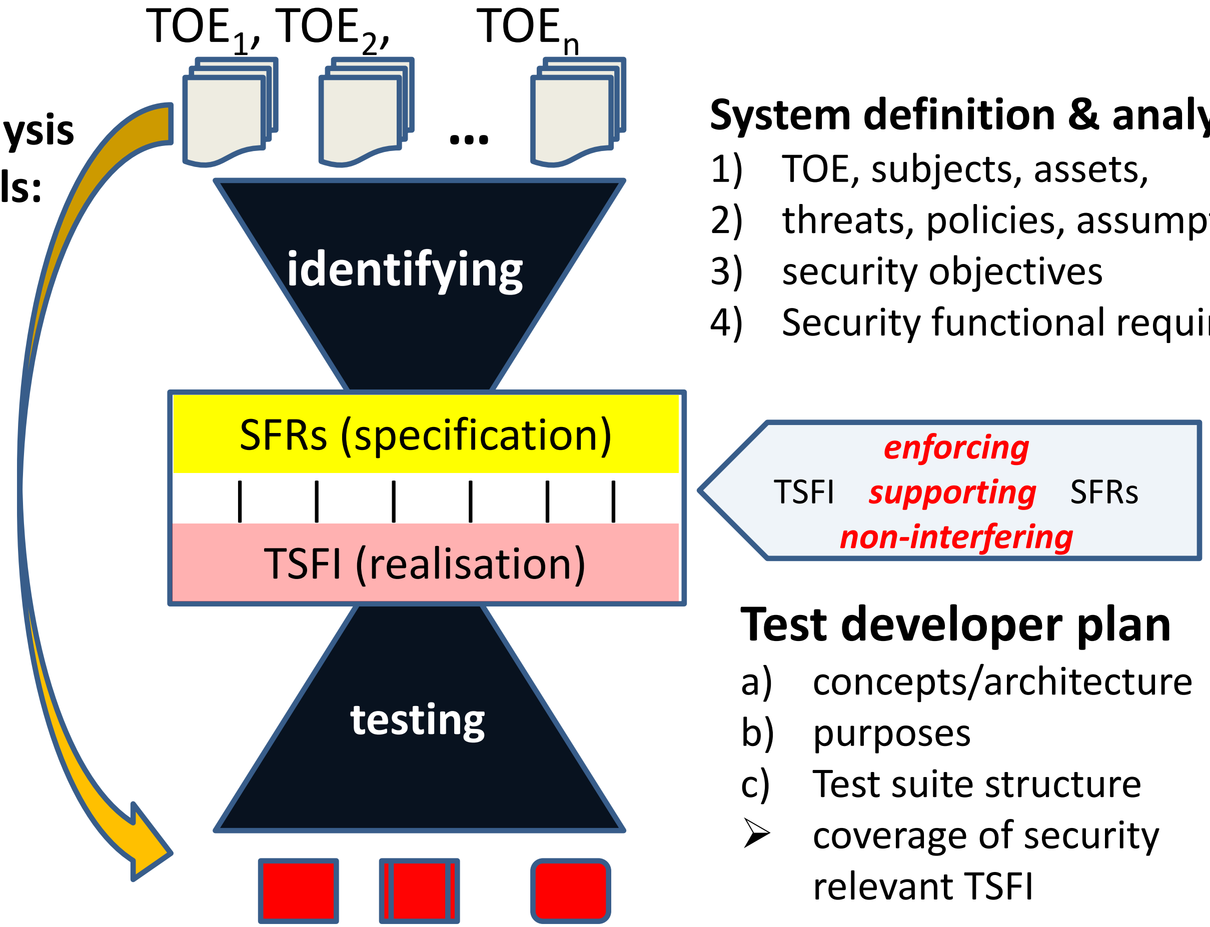
To be approved

(2) Model-based security testing

System (risk) analysis methods & models:
e.g. CORAS, UMLsec

usecase
▼
testcase

Test tools & techniques:
e.g. fuzzing, partitioning



TCL, JUnit, C++, TTCN-3, manual tests…

System definition & analysis

1) TOE, subjects, assets,
2) threats, policies, assumptions
3) security objectives
4) Security functional requirements

Test developer plan

a) concepts/architecture
b) purposes
c) Test suite structure
➢ coverage of security relevant TSFI

(2) Experiences from case studies

- Risk-based testing **(Banking, Automotive):**
  - Risk-based test identification & risk-based test selection
- Advanced fuzz testing **(Banking, Radio Protocols, Automotive, Telecom, Industrial Automation):**
  - Model-based behavioural fuzzing
  - Model inference assisted smart fuzzing
- Active testing techniques **(Banking, Radio Protocols)**
  - Model-based security testing from behavioral models and test purposes
  - Active intrusion testing
- Autonomous testing techniques **(Radio Protocols, Industrial Automation):**
  - Events-based passive testing/monitoring
  - Anomaly detection with machine learning

(2) Industrial experiences (ToC)

- **Case Study (sample structure)**
  - Characteriazation
    - Background (challenges)
    - System under Test
    - Risk Analysis
  - Security Testing Approaches
    - Applied approaches
    - Comparison with So niques
  - Results so far
    - Expectati
    - Test Resul
  - Exploitation (value of techniques)
- Assessment criteria (metrics) for all case studies

Under development

(3) Security design guide (V&V)

- Security design guide enabling test and assurance (V&V)
  - ***Focus on the design phase***
  - ***Guidance to system designers*** *that* ***supports verification and validation*** *across the lifecycle*
  - *Consideration of* ***requirements for (later) testing (phase)*** *during design phase*
- Following ISO/IEC 15288 (System lifecycle processes) from SC7

(3) V&V (EG 201 581) ToC

- The security design lifecycle
  - **Scope, References**
  - **Definitions, symbols and abbreviations**
  - **Security in the Lifecycle (lifecycle stages)**
  - **Security design activities (process step**
  - **Tools and methods mapping to lif ges and security processes**

  - Annex A: Security contex nciples
  - Annex B: Security Ar l Components
  - Annex C: Applicati ommon criteria in security standardisation
  - Annex D: Application of security assurance profile in security standardisation

Under development

Time plan

- Terminology document (TS 101 583)

  to be published in summer 2013

- Case study experience (TS 101 582)

  to be published 2nd half 2013

- V&V (EG 201 581)

  to be published 2nd half 2013

- Future liaison with SC27/WG3

  to be esthablished

  to exchange/comment working draft standards