ARMOUR

# Model-Based Security Testing for IoT Labelling & Certification

**Elizabeta Fourneret** (Smartesting)
Panos Karkazis (SYNELIXIS)

ReCRED, Clustering Workshop, Athens, Greece

2018, January 31st

www.armour-project.eu

# Contribution for IoT Labelling and Certification

1. **How to make the testing part of the labelling and certification process cheaper ?**
   - Approach **Easy to use** by certification bodies and **extensible**
   - Build on reusable, configurable security test patterns and automated test generation
   - The certification scheme comes with the test patterns to be used

2. **How to ensure the quality and reproducibility of the assessment?**
   - The **security test patterns** should be agreed by the certification authorities
   - Test automation ensure the replicability of the results

3. **How to deal with change?**
   - Using the **automated testing** for continuous monitoring and testing at running stage to keep the certificate alive

# ARMOUR in a nutshell

**Duration** 24 months (from Feb 2016 to Jan 2018)

**EU funding** 2 Millions €

**Consortium** 8 partners including 5 SMEs, 1 university and 2 research centres

# Challenges of IoT Security & Trust

ARMOUR

*Business Logic Vulnerabilities*

*Uncertainty of the expected behaviour of IoT systems*

*Large-scale dimension, heterogeneity, compositionality and dynamic configuration of IoT systems*

*Ensuring End-to-End Security & Privacy Testing*

# MBST Process

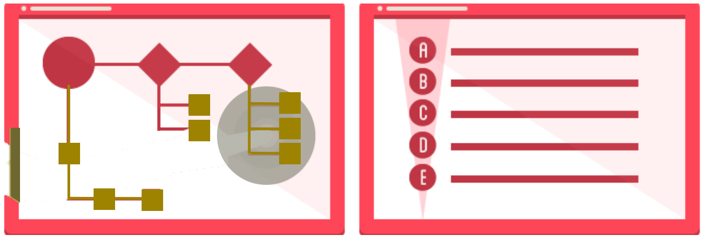
Security needs & requirements

Security Test Objectives

Risk Analysis

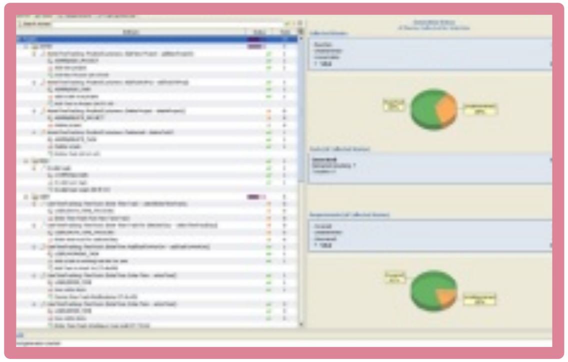
Security Test Patterns

Modeling for test generation




MBT Tool

Automatic test generation



Test Repository (TTCN-3, Java…)

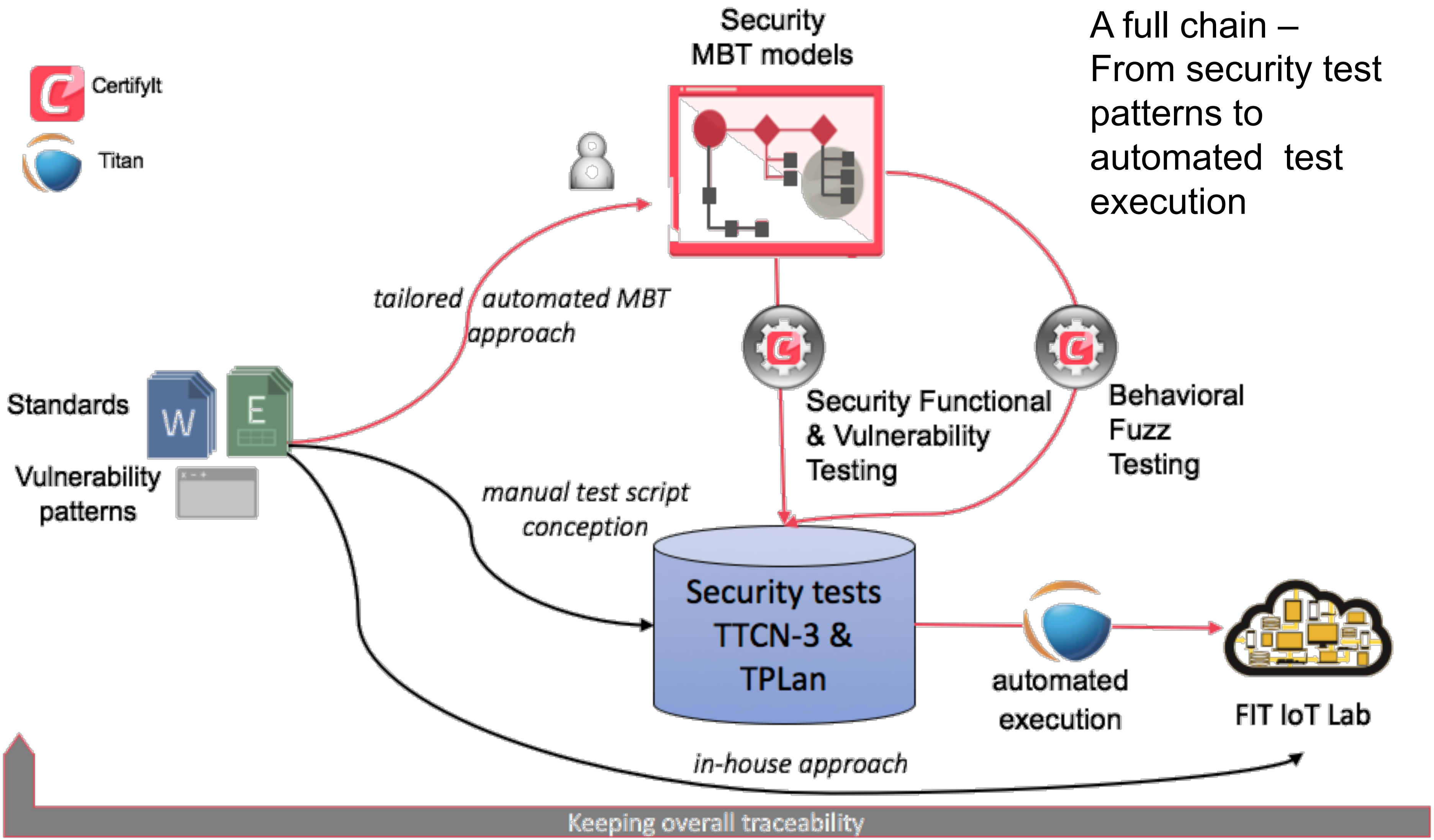
Security tests

Manual execution

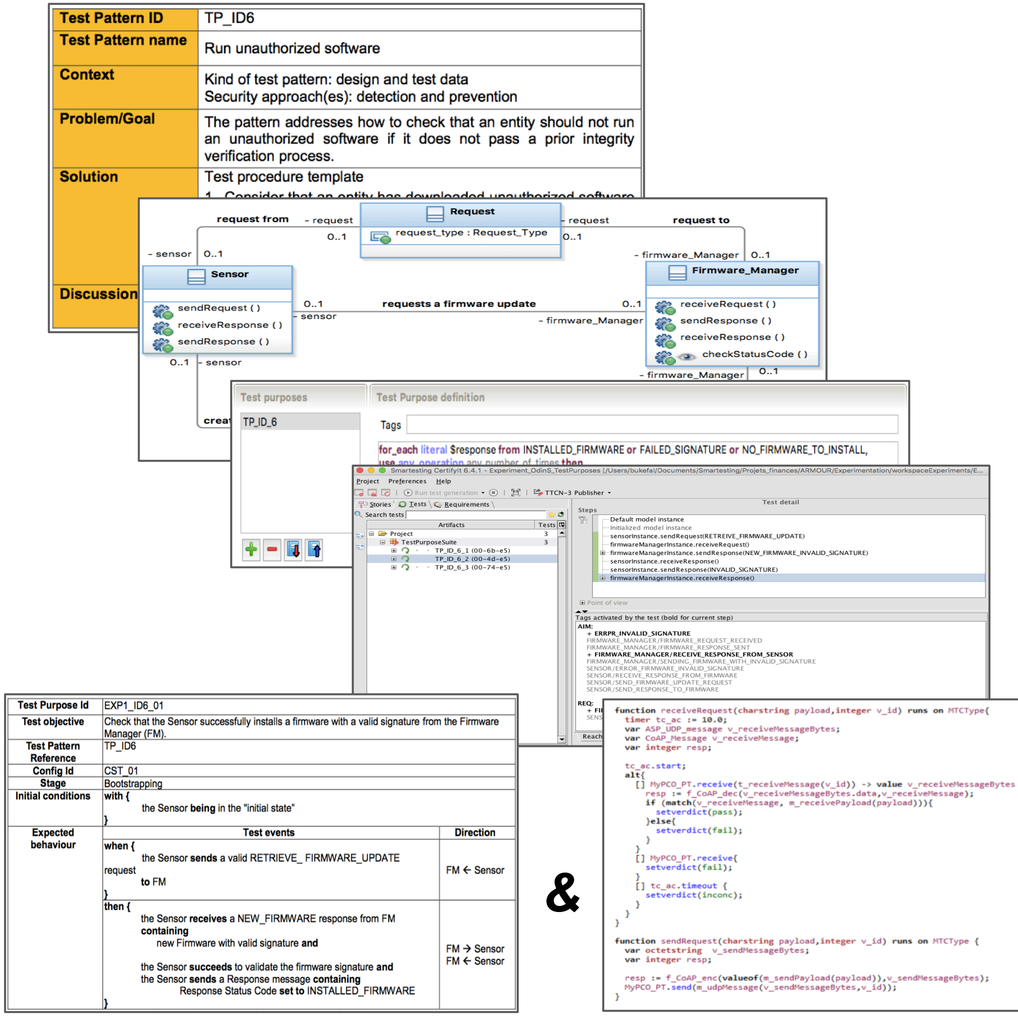
& scripts for automation

# ARMOUR Testing Framework

A full chain –
From security test patterns to automated test execution



# MBST Approach in 5 steps




① **_Vulnerability Analysis_**

② **_Extracting API & Model Inference_**

③ **_Security test pattern selection_**

④ ***MBT test generation*** *based on ARMOUR test strategies*

⑤ ***Publication*** *in* ***TPLan*** *– test description and* ***TTCN-3*** *test scripts*

*Test results & Labelling analysis*

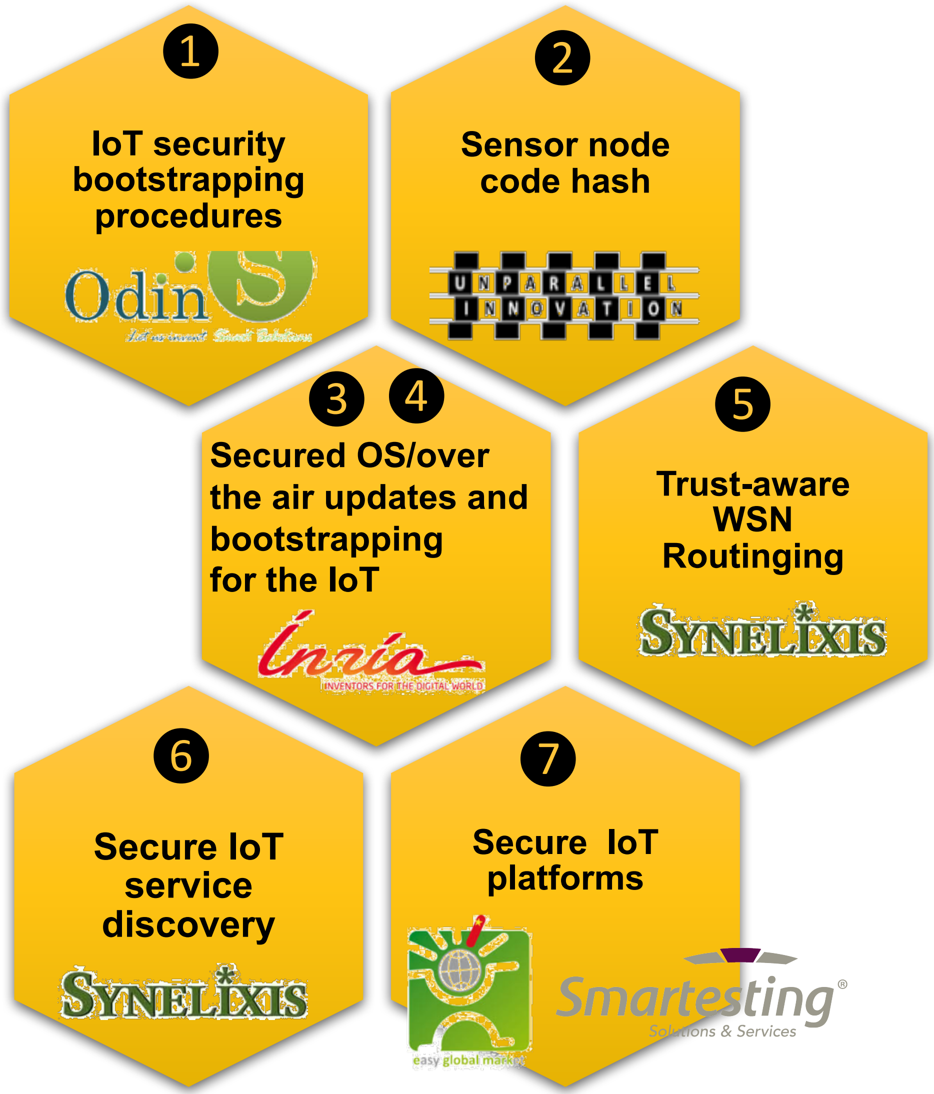
# Outline

1. ARMOUR Project : Challenges and Objectives
2. Model-Based Security Testing
   – Approach & contribution for IoT Labelling and Certification
3. Experiments
4. Conclusion

# Seven IoT Security & Trust experiments

7 experiments covering complementary **segments of an IoT deployment**:

- Devices and data → 1, 2 & 3
- (Wireless) connectivity → 4 & 5
- Applications & Services → 6
- Platforms → 7

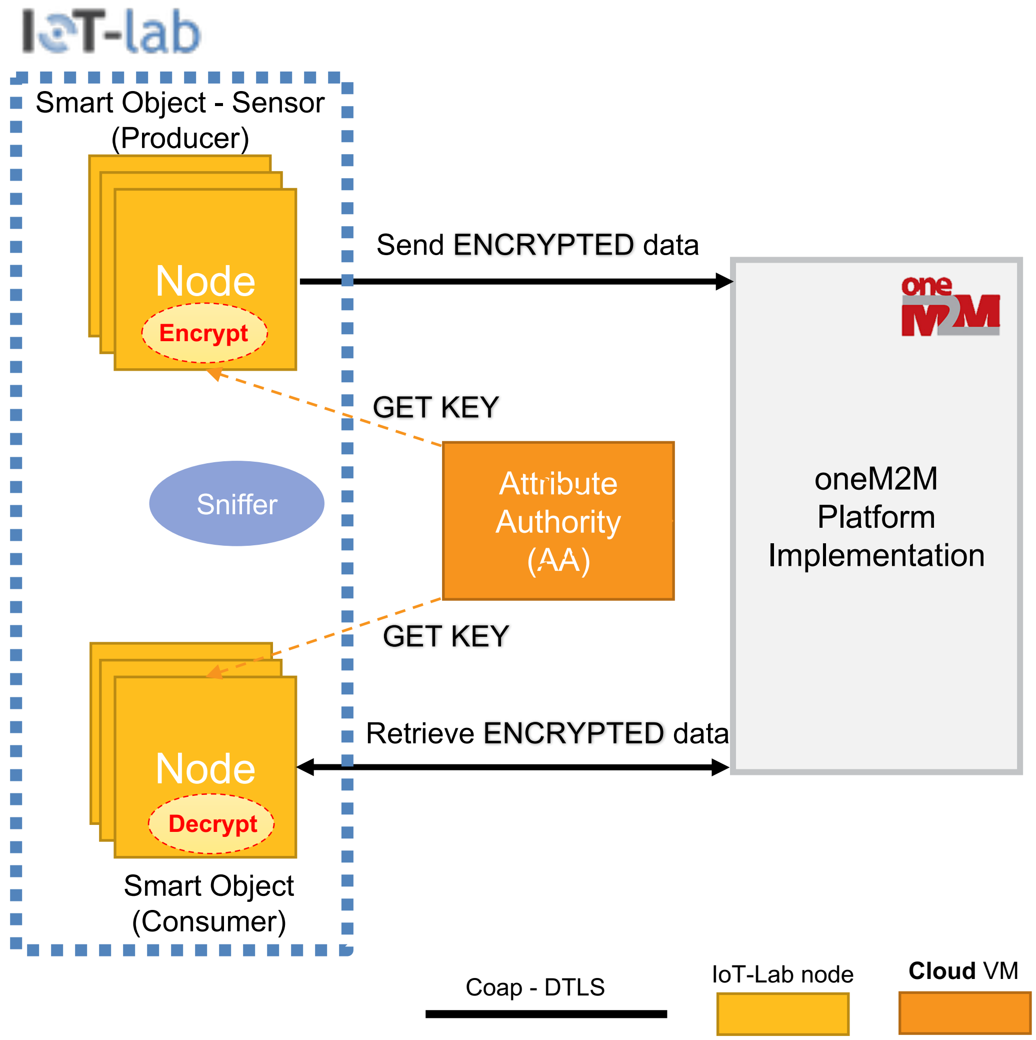



*Test and validation of the framework*

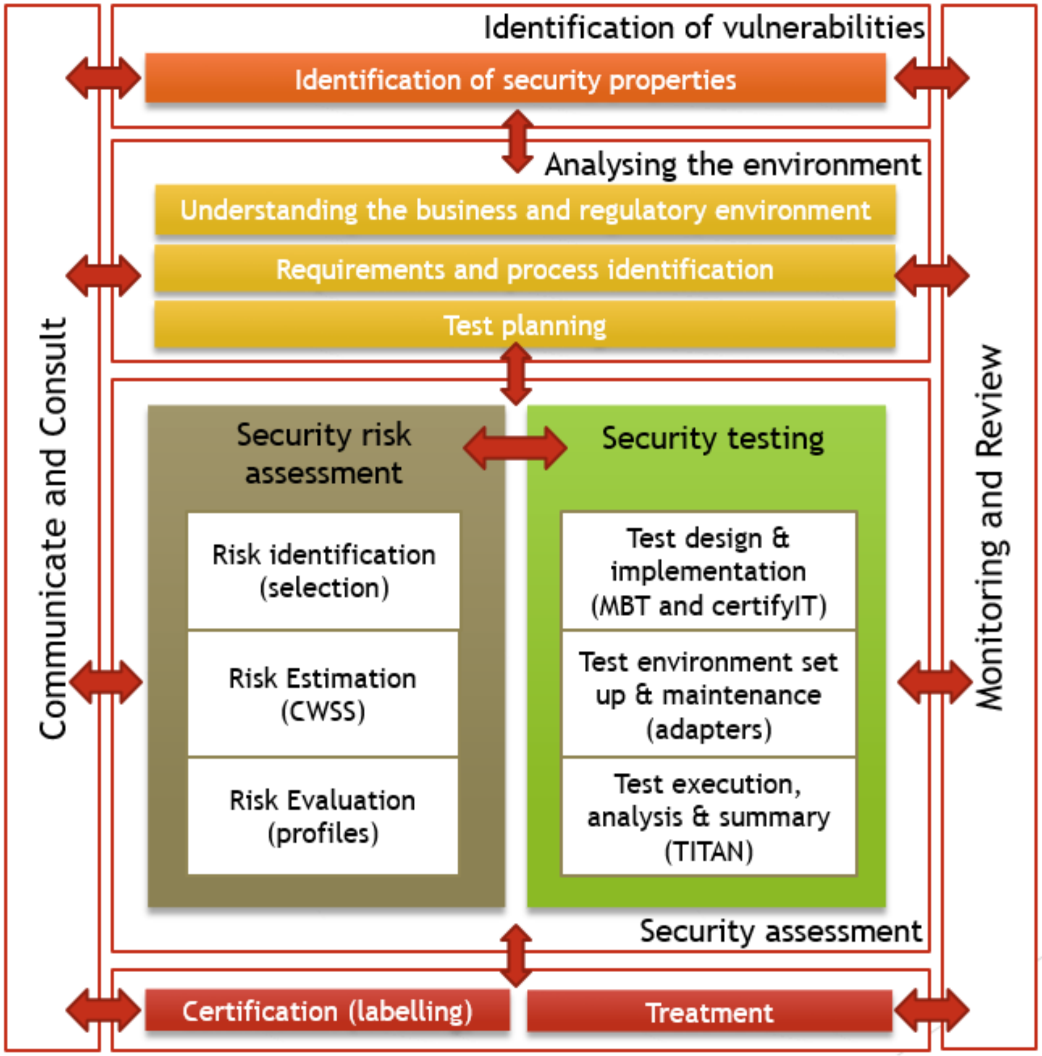
*Contribution to testing campaigns*

# Large-Scale & End-2-End Case Study (Example)

| TP ID | Security Test Patterns |
|---|---|
| **TP_ID6** | Run unauthorized software |
| **TP_ID8** | Resistance to eaves dropping and man in the middle |
| **TP_ID10** | Resistance to Injection Attacks |
| **TP_ID11** | Detection of flaws in authentication |



# Follow the ETSI approach and ISO 31000




ETSI, “Methods for testing & specification; risk-based security assessment and testing methodologies,” 2015

# Identification of vulnerabilities

ARMOUR

- Database of general security threats in IoT (not included in ISO 31000)
- Compact threats of OneM2M to simplify and adapt to IoT devices also

| | |
|---|---|
| Lack of Authentication | • The endpoints should be legitimate. |
| Replay attack | • Intermediate entity can store a data packet and replay it at a later stage. |
| Insecure cryptography | • The cryptographic suite and key length must be enough to avoid certain type of attacks,<br>• such as dictionary attack or force brute. |
| DoS attacks | • Several endpoints can access to the server at the same time in order to collapse it. |
| Lack of Integrity | • Received data are not tampered with during transmission; if this does not happen, then any change can be detected. |
| Lack of Confidentiality | • Transmitted data can be read only by the communication endpoints. |
| Lack of Authorization | • Endpoint services should be accessible to endpoints who have the right to access them. |
| Lack Fault tolerance | • Exceptions should be controlled to avoid faults that affects the endpoints. |

# Security testing

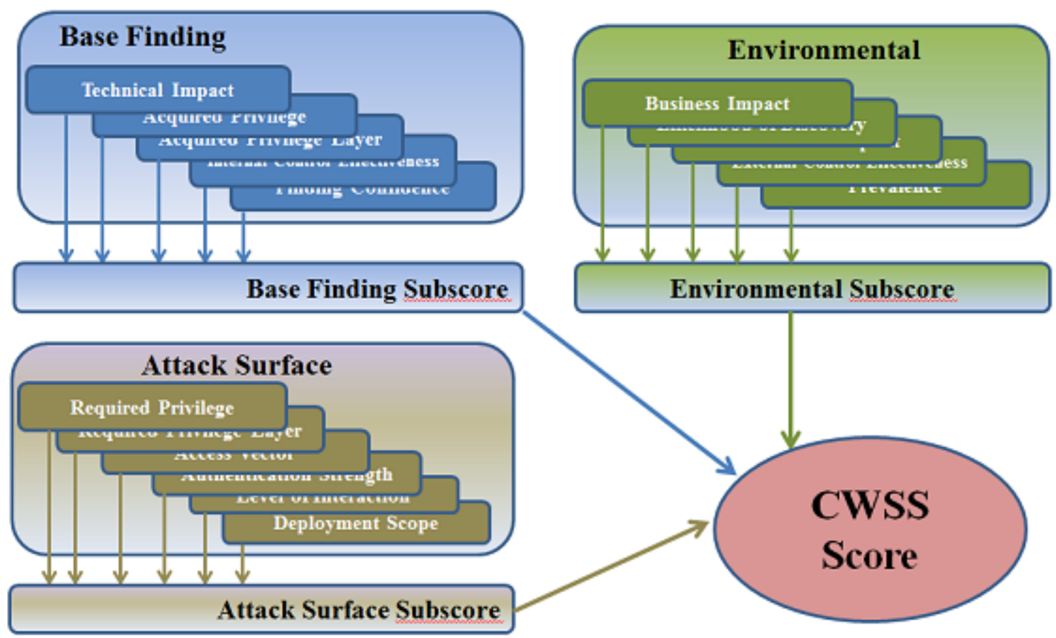
- From the vulnerabilities considered in the first phase, we produce security tests
- In the ETSI proposal, the automation of this phase is not contemplated, but the automation of this process eases the update of the label to cope with changing conditions in which the device operates.
- In ARMOUR project, this process is intended to be **automatized**:

- The tests provide us a series of security metrics such as % of ciphered data, % of messages protected against replay attack, etc. The different general tests are shown in the figure of mapping with OneM2M (relation).

# Security risk assessment

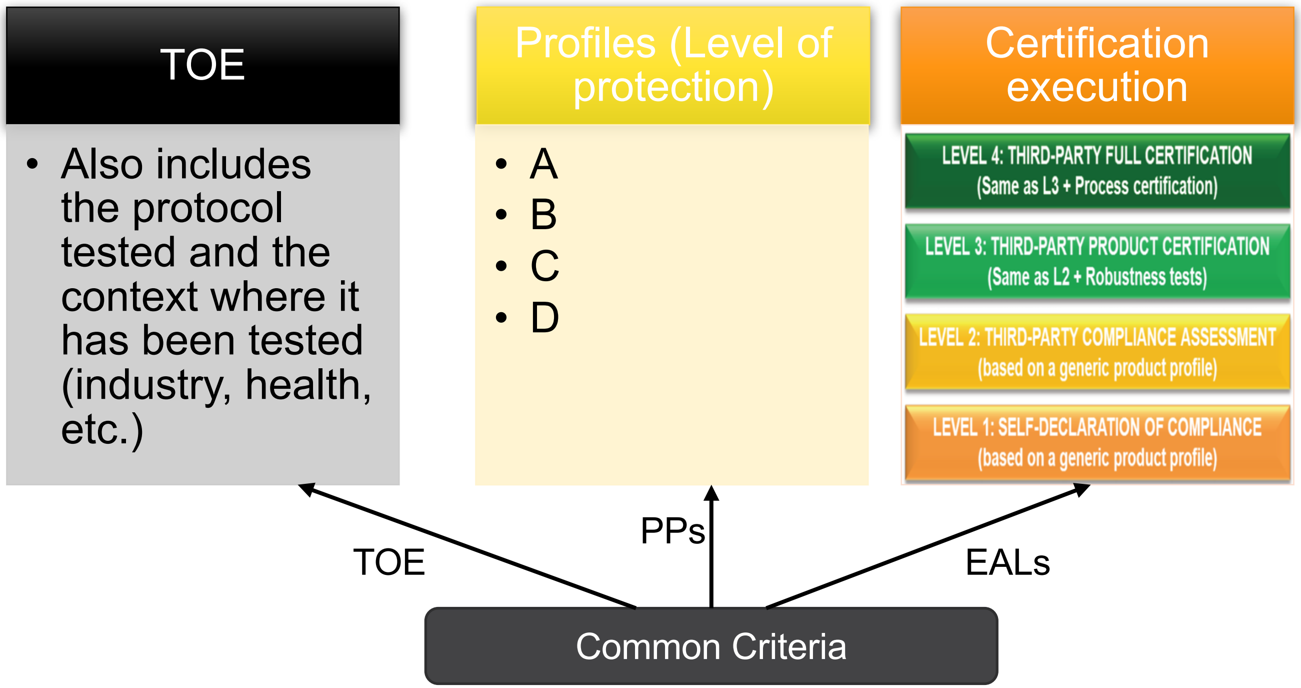
- The CWSS metrics can be obtained:
  - From testing
  - By default taking into account the vulnerability
  - By default if they are not applicable to IoT or to our certification procedure (e.g finding confidence, since the scenario is evaluated before being attacked) (*Risk Identification phase*)
- *Risk Estimation phase*: we calculate the score for each vulnerability by means of the CWSS formula:

S= BF * AS * ES



# Certification - Labelling

- As an output of the general certification process, we obtain a label associated to the risk of the scenario tested.
- Three mains aspects are considered to be included in the label, following the Common Criteria approach



# Certification - Labelling

- Visual labelling following the recommendations of ENISA and ECSO. The result of the evaluation need to be communicated appropriately to the user.
- Multidimensional, like security.
- To perform a fast labelling update, we propose the usage of a QR.

# Conclusion : On the way to MBST for IoT Systems Labelling & Certification

ARMOUR

**Security is number one challenge in the IoT domain**

ARMOUR

- **Model-Based Security Testing as a core technology to ensure a trustable labelling scheme**

- **Domain-specific modeling**
- **Machine learning algorithms**

ARMOUR

**Towards a Trust Label Process**
supported by (large scale) IoT enhanced security test-beds

ARMOUR

**Collaborations & contributions**

oneM2M

AIOTI

IERC

ARMOUR

ARMOUR

www.armour-project.eu

**ARMOUR - Large-Scale Experiments of IoT Security Trust**

| Call Identifier | Topic | Project Reference | Type of Action |
|---|---|---|---|
| H2020-ICT-2015 | ICT-12-2015 Integrating experiments and facilities in FIRE+ | 688237 | RIA - Research and Innovation action |

**Start date of the project** February 1st, 2016

**Duration** 24 months

UPMC SORBONNE UNIVERSITÉS · Inria INVENTORS FOR THE DIGITAL WORLD · SYNELIXIS · Smartesting Solutions & Services · UNPARALLEL INNOVATION · European Commission · easy global market · OdinS Let us invent Smart Solutions