20

ARMOUR

20.1 Project Objectives

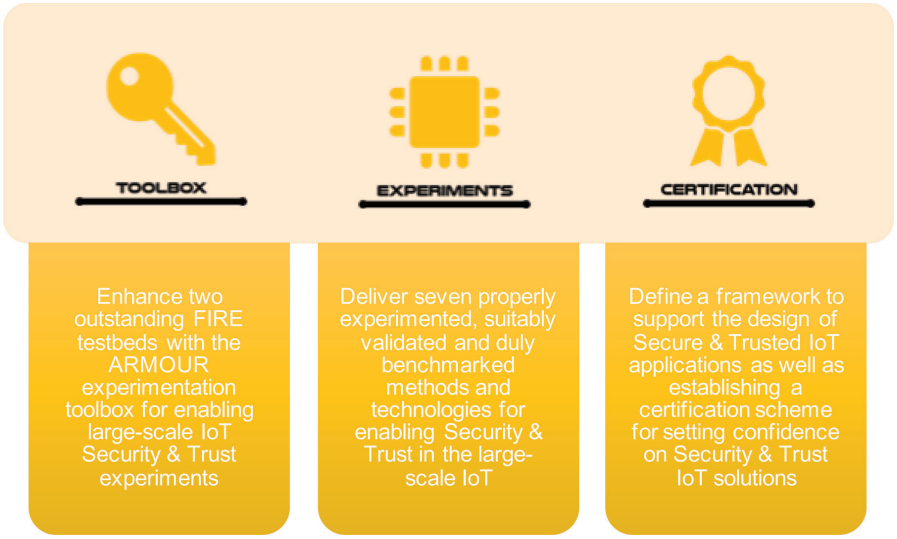
Large-scale and distributed systems are good examples where the experimental approach is necessary. Such systems are built using very advanced features that have several multi-level interlinks/dependencies, which make it very difficult to analyse and predict the system overall behaviour. The runtime environments play a very important role in the overall performance and even different implementations of the same standard can impact their behaviour. Moreover, in large-scale distributed systems, the picture even more complex with the different resources potentially being heterogeneous, hierarchical, distributed or dynamic. Finally, failures, shared usages, etc. make the behaviour of large-scale distributed systems hard to predict[1]. The large-scale distributed Internet-of-Things (IoT) is a case where an experimentation (research) approach is required to have proper guarantee on its solutions.

The central goal of the ARMOUR project is then to perform large-scale experimentally-driven research as the way to provide properly tested Security & Trust solutions for large-scale IoT. "*Experiment is a test under controlled conditions that is made to demonstrate a known truth, examine the validity of a hypothesis, or determine the efficacy of something previously untried*"[2]. The ARMOUR experiments are aimed at determining the efficacy and performance of key Security & Trust methods in a large-scale distributed Internet-of-Things.

[1] Jens Gustedt, Emmanuel Jeannot, and Martin Quinson. Experimental Methodologies for Large-Scale Systems: A Survey. Parallel Processing Letters 2009 19:03, pp. 399–418.

[2] Experiment. (n.d.) American Heritage® Dictionary of the English Language, Fifth Edition. (2011). Retrieved April 10 2015 from http://www.thefreedictionary.com/experiment

ARMOUR identified 3 goals that define the approach being used to achieve the proposed Security and Trust solutions:



In testing and experimentation one often uses the term "large-scale" to denote an environment that exceeds the size, scope and capabilities of a laboratory environment. The notion of scale could not refer to the number of artefacts, whether these are switches, routers, computing nodes, sensors, cars, homes, etc. "Scale" can refer to the scope or extent of experimentation and "large" can imply heterogeneity based on the assumption that large-scale exceeds the borders of a single laboratory setting. "Large-scale" usually qualifies as in the upper thousands for sensors/small devices, or in the scope of routing nodes in the lower hundreds[3]. ARMOUR will perform large-scale experiments involving one-to-two thousand heterogeneous devices made available by a large-scale FIRE IoT facility – the FIT IoT-LAB testbed – that has been enhanced for supporting Security & Trusted experimentation.

Furthermore, a good experimentation implies verifying the repeatability, reproducibility, and reliability conditions in order to ensure generalisation of experimental results, and verifiability of their credibility. A proper experimentation methodology will be implemented, technologies subject to

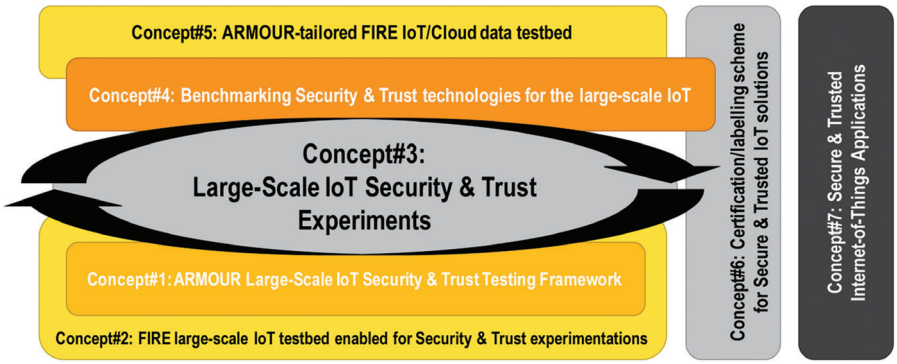
[3]Experimentally driven research white paper, FP7-224524 FIRE Fireworks Support Action, April 2010.

experimentation will be benchmarked and even a new certification scheme will be designed for providing a "quality" label for large-scale IoT Secure & Trusted solutions. Also, applications of large-scale IoT Security & Trust will be studied and design guidance will be established for developing applications that are Secure and Trusted for the large-scale Internet-of-Things.

Finally, data and benchmarks from experiments will be properly handled, kept and made available via a FIRE data IoT facility – the FIESTA IoT/Cloud infrastructure. The FIESTA facility will be adapted and configured to hold the ARMOUR experimentation data and benchmarks. In this way, research data is properly preserved and made available to the research communities also making possible to compare results with experiments performed in other testbeds and/or also to confront results of disparate Security & Trust technologies.

20.2 Project Concept

In the following, we present a picture outlining the general main concepts subjacent to ARMOUR, and a brief description of the 7 concepts that shape the ARMOUR project. A detailed in-depth description of each of these concepts follows right after in the next sub-sections of this document.



- **Concept#1: ARMOUR Large-Scale IoT Security & Trust Testing Framework**. Security & Trust Experimentation on a large-scale Internet-of-Things brings some critical challenges for software testing techniques, concepts and tools in terms of business logic vulnerabilities, expected behaviour of IoT systems and the dimension, heterogeneity, compositionality and dynamicity of IoT systems. Presently no testing framework

exists to cope with these challenges. ARMOUR will create a large-scale IoT Security & Trust testing framework that can be adapted easily to the various domains and experimented on the testbeds provided by the FIRE initiative and beyond.

- **Concept#2: FIRE large-scale IoT testbed enabled for Security & Trust experimentations**. ARMOUR takes advantage of the unique FIRE FIT IoT-LAB for validating research results under large-scale real life conditions fostering the design and deployment of IoT Security & Trust solutions. For this, the IoT-LAB testbed will be enhanced with the ARMOUR Large-Scale IoT Security & Trust Testing Framework. The IoT-LAB testbed provides a unique open first class service to all IoT developers, researchers, integrators and developers: a large-scale experimental testbed allowing design, development, deployment and testing of innovative IoT applications. It offers a first class facility with thousands of wireless nodes to evaluate and experiment very large scale wireless IoT technologies ranging from low level protocols to advanced services integrated with Internet, accelerating the advent of ground-breaking networking technologies.
- **Concept#3: Large-Scale IoT Security & Trust Experiments**. With the FIRE FIT IoT-LAB ready for large- scale IoT Security & Trust experimentations it is possible then to perform the central goal of the project – the ARMOUR Large-Scale IoT Security & Trust Experiments. A set of experiments has been brought forward by the project partners (majorly by SMEs) based on their specific interests of technological performance improvement and/or innovation. These experiments will follow a well-defined methodology as to ensure reproducible, extensible, applicable and revisable experimentations. Experimentation process will be iterative in order to maximise solutions' efficacy.
- **Concept#4: Benchmarking Security & Trust technologies for the large-scale IoT**. It is a major necessity to provide tools for IoT stakeholders to evaluate the level of preparedness of their system to IoT security threats. Benchmarking is the typically approach to this and ARMOUR will be the first to establish a security benchmark for end-to-end security in the large-scale IoT. A new methodology for benchmarking Security & Trust technologies for IoT will be conceived (especially considering large-scale conditions) that will go beyond traditional approaches for security benchmarking by building up on the ARMOUR large-scale testing framework and process. And, the ARMOUR experiments will be benchmarked using the ARMOUR benchmarking methodology.

- **Concept#5: ARMOUR-tailored FIRE IoT/Cloud data testbed**. ARMOUR takes advantage of the FIESTA IoT/Cloud testbed to make experimentation and benchmarking data duly available, preserved, able to be inspected and visualised, and also making possible to compare data of experiments from disparate IoT testbeds. The FIESTA IoT/Cloud testbed provides access to and sharing of IoT datasets in a testbed-agnostic way and enables portability of IoT experiments across different testbeds, through the provision of interoperable standards-based IoT/cloud interfaces over disparate IoT experimental facilities. FIESTA implements a new first-of-a-kind meta-testbed that enables the execution of experiments that exploit data and resources from multiple underlying federated testbeds.
- **Concept#6: Certification/labelling scheme for Secure & Trusted IoT solutions**. Certification is a key element to support a specific level of trust on a (large-scale) IoT infrastructure/technology because the presence of non-certified IoT solutions/products could be open to vulnerabilities. ARMOUR will establish a rigorous certification scheme for labelling an IoT device/system with respect to (large-scale) Security & Trust. The ARMOUR benchmarking framework will be used as a basis for the certification activities so that IoT technologies and deployments could apply for a certificate to prove its security level toward third parties.
- **Concept#7: Secure & Trusted Internet-of-Things Applications**. It is fundamental to understand how security and privacy solutions are able to support the lifecycle of IoT applications. Particularly, how different security and privacy solutions or components, which are defined in their respective systems or contexts, can be used in a harmonised way to support the design and deployment of secure IoT applications. To this, ARMOUR will create procedures to test and validate the migration and the extendibility of IoT applications from the security and privacy viewpoints especially considering uses in a large-scale Internet-of-Things, e.g. considering the migration aspects (from one release to another of the IoT application) or the level of crypto-agility and flexibility, etc.

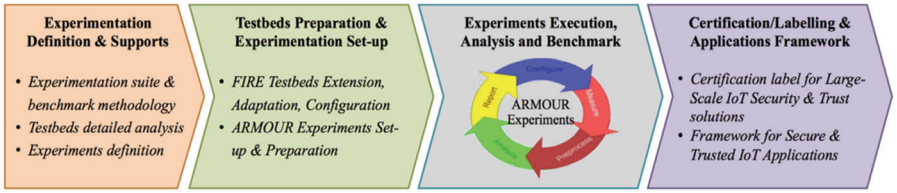
20.3 Project Approach

The ARMOUR project considers a large-scale experimentally-driven research approach. The large-scale distributed Internet-of-Things is a case where an experimentally-driven approach is required due to its high dimensionality,

multi-level interdependencies and interactions, non-linear highly-dynamic behaviour, i.e. due to its complex nature. The large-scale experimentally-driven research approach makes possible to experiment and validate research technological solutions in large-scale conditions and very close to real-life environments.

The ARMOUR large-scale experimentally-driven approach is realised by a well-established methodology for conducting good experiments that are reproducible, extensible, applicable and revisable. The methodology aims at verifying the repeatability, reproducibility, and reliability conditions to ensure generalisation of experimental results, and verifiability their credibility.

The general steps of the ARMOUR methodology encloses generically four steps: (1) Experimentation Definition & Supports; (2) Testbeds Preparation & Experimentation Set-up; (3) Experiments Execution, Analysis and Benchmark; (4) Certification/Labelling & Applications Framework. The figure below depicts the methodology.



Step 1 – Experimentation Definition & Supports

The first step marks the start of the experimentation process and relates to the detailed definition of the ARMOUR experiments and the supports for experimentation (namely the Experimentation Suite and the Benchmarking Framework). This step basically involves:

- Definition of the IoT Security & Trust experiments (including defining testing scenarios, needed conditions, analysis dimensions) and the technological architecture for ARMOUR experimentations;
- Research and development of the ARMOUR technological experimentation suite and benchmarking methodology for executing, managing and benchmarking large-scale Security & Trust IoT experiments;
- Analyse the FIT IoT-LAB testbed and FIRE FIESTA IoT/Cloud testbed for assessing their specific composition, supports and services in view of the ARMOUR IoT Security & Trust experimentations.

Step 2 – Testbeds Preparation & Experiments Set-up
The second set of the experimentation methodology relates to establishing the proper conditions of conducting IoT Security & Trust experimentations using the selected testbeds and preparing the experiments. This step involves:

- Extending, adapting and configuring testbeds to enable IoT large-scale Security & Trust experiments:
  - Enhance FIT IoT-LAB testbed with the ARMOUR experimentation suite and, adjust/tune the testbed for multi-scenario large-scale IoT large-scale Security & Trust experiments;
  - Adapt and configure the FIRE FIESTA IoT/Cloud testbed for adequately supporting IoT Security & Trust experimentation data and benchmarks from ARMOUR large-scale experiments;
- Setting-up and preparing the ARMOUR experiments by specifying the security & trust test patterns for the experimentation that will then be used to execute and manage the experiments.

Step 3 – Experiments Execution, Analysis and Benchmark
The third step of the experimentation process relates to the actual execution of the ARMOUR experiments that represents the core research of the project to achieve the proven Security & Trust solutions for large-scale Internet-of-Things. This step takes the following sub-steps (iteratively):

- Configure – Install the scenario(s) for IoT large-scale Security & Trust experimentation;
- Measure – Do the measurements and collect the data from the ARMOUR experiments;
- Pre-process – Preform pre-processing and organisation of stored experimentation data;
- Analyse – Analyse data, do experiments benchmarking and compare performance;
- Report – Report on experimentation results (and possibly publish them even).

Step 4 – Certification/Labelling & Applications Framework
The final phase of the ARMOUR methodology relates to the creation of the certification label for large-scale IoT Security & Trust technologies and the establishment of a framework for Secure & Trusted IoT applications. These related especially with:

- A framework to define how different security & privacy solutions or components, defined in their respective systems or contexts, can be used to support the design/deployment of secure IoT applications;
- A new labelling scheme for high-dimensional Secure & Trusted Internet-of-Things solutions that provides the needed user and market confidence on their deployment, adoption and use.