ARMOUR Project aims to address Security and Trust issues on Internet of Things by providing duly tested, benchmarked and certified Security & Trust technological solutions for large-scale IoT using upgraded FIRE large-scale IoT/Cloud testbeds properly-equipped for Security & Trust experimentations. And to enable ARMOUR to successfully achieve its objectives, the project image and dissemination materials play an important role. This Deliverable includes the dissemination materials created for ARMOUR’s outreaching activities. It starts with the definition of the ARMOUR brand, which includes the Project Logotype, in different versions so it can be used in different circumstances and with different backgrounds, and a description of the official colours used in the ARMOUR Logotype. This deliverable also provides the layout design & templates, for the posters, flyers, website, stationary and slides. Afterwards, the already existing dissemination materials are presented (created until month 6) including the project website, project posters (including a project overview and some specific ones dedicated to the internal experiments that will be conducted within the project), project flyers and project website.

Disclaimer

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 688237, but this document only reflects the consortium’s view. The European Commission is not responsible for any use that may be made of the information it contains.
## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>17/06/2016</td>
<td>Creation of the Table of Contents</td>
<td>UI</td>
</tr>
<tr>
<td>0.2</td>
<td>01/07/2016</td>
<td>Added Dissemination Strategy &amp; ARMOUR Branding</td>
<td>UI</td>
</tr>
<tr>
<td>0.3</td>
<td>15/07/2016</td>
<td>Added Experiments Posters</td>
<td>All partners</td>
</tr>
<tr>
<td>0.4</td>
<td>22/07/2016</td>
<td>Final Draft for Internal Review</td>
<td>UI</td>
</tr>
<tr>
<td>1.0</td>
<td>28/07/2016</td>
<td>Proof-reading and minor corrections</td>
<td>UPMC</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Introduction ................................................................................................................... 5  
   1.1 ARMOUR project ................................................................................................... 5  
   1.2 The role of WP5 in ARMOUR ................................................................................ 5  
   1.3 Dissemination Strategy .......................................................................................... 6  
   1.4 Purpose of this deliverable .................................................................................... 7  

2 ARMOUR: The brand ................................................................................................... 8  
   2.1 ARMOUR Logo ...................................................................................................... 8  
      2.1.1 Logo Variants ................................................................................................. 9  
      2.1.2 Protection areas of the ARMOUR logo ........................................................... 9  
   2.2 Official colours ..................................................................................................... 10  
   2.3 Layout Design & Templates ................................................................................. 11  
      2.3.1 Stationary ..................................................................................................... 11  
      2.3.2 Website ........................................................................................................ 15  
      2.3.3 Document Layout ......................................................................................... 18  
      2.3.4 Slides Template ............................................................................................ 19  
      2.3.5 ARMOUR Banner ......................................................................................... 25  

3 Dissemination Posters ................................................................................................ 26  
   3.1 What is ARMOUR? .............................................................................................. 27  
   3.2 ARMOUR Experiments ........................................................................................ 28  

4 Project Website ........................................................................................................... 35  

5 Flyer ............................................................................................................................ 50  

6 Conclusion .................................................................................................................. 52  

7 Bibliography ................................................................................................................ 53
1 Introduction

1.1 ARMOUR project

The Internet-of-Things (IoT) is rapidly heading for large scale meaning that all mechanisms and features for the future IoT need to be especially designed and duly tested/certified for large-scale conditions. Also, Security, Privacy and Trust are critical elements of the IoT where inadequacy of these is a barrier to the deployment of IoT systems and to broad adoption of IoT technologies. Suitable duly tested solutions are then needed to cope with security, privacy and safety in the large scale IoT. Interestingly, world-class European research on IoT Security & Trust exists in European companies (especially SME) and academia where even there are available technologies that were proven to work adequately in the lab and/or small-scale pilots. More, unique experimental IoT facilities exist in the EU FIRE initiative [1] that make possible large-scale experimentally-driven research but that are not well equipped to support IoT Security & Trust experiments. But notably, Europe is a leader in IoT Security & Trust testing solutions (e.g. RASEN toolbox [2], ETSI Security TC [3], etc.) that can be extended to large-scale testing environments and be integrated in FIRE IoT testbeds for supporting experimentations. The ARMOUR project is aimed at providing duly tested, benchmarked and certified Security & Trust technological solutions for large-scale IoT using upgraded FIRE largescale IoT/Cloud testbeds properly-equipped for Security & Trust experimentations. To this, ARMOUR:

1. Enhance two outstanding FIRE testbeds (> 2700nodes; ~500users) with the ARMOUR experimentation toolbox for enabling large-scale IoT Security & Trust experiments;
2. Deliver six properly experimented, suitably validated and duly benchmarked methods and technologies for enabling Security & Trust in the large-scale IoT;
3. Define a framework to support the design of Secure & Trusted IoT applications as well as establishing a certification scheme for setting confidence on Security & Trust IoT solutions.

1.2 The role of WP5 in ARMOUR

This work package deals with the important outreaching activities of the ARMOUR project. In particular, it tackles:

- The planning and execution of dissemination activities that will increase the awareness of the ARMOUR project;
- The exploitation strategic planning and activities for ARMOUR exploitable assets;
- The collaboration with other relevant projects and the participation in clustering activities on FIRE, IoT and Security related clusters.
1.3 Dissemination Strategy

ARMOUR has a clear strategy in terms of dissemination activities, and this strategy can be clearly identified in the next figure. It shows that the dissemination strategy of ARMOUR is made up of three consecutive phases. The three phases of dissemination require different methods and activities to be undertaken in order to achieve their goals. The details of the phases are as follow:

### Awareness-Oriented phase

At the start of project, the goal of this phase is to raise public, industry and research community awareness about the project and the problems that it aims to tackle. During this phase of the dissemination, the tasks involve the setting up of the basic marketing materials and awareness-raising presentations at different related events. Thus, the main activities will be the following:

- Setting up a common project design, such as the ARMOUR logo, templates for documents and presentations;
- Creating the project website, which will describe the challenges and goals of the project and will present the project members;
- Designing the project information materials (such as flyers and posters), which will be distributed through partners’ networks, project events and published on the project website;
- Giving introductory presentations at conferences and workshops about the challenges and goals of ARMOUR in order to raise awareness amongst scientific and industry stakeholders and to establish the basic brand name of ARMOUR.

### Result-Oriented phase

The aim of this phase is to promote project results. During this dissemination phase, results of the ARMOUR project will be published to promote these to stakeholders in internet system domains: research centres, industry and users, whilst also paying attention to SMEs and small research teams. The planned activities are:

- Establish technical sustainability (i.e. benchmark)
- Identified interested parties
- Prepare exploitation
• Update the project website with public deliverables and news in order to show the liveness and progress of the project and to keep interested parties up-to-date;
• Presentations at international conferences and workshops introducing the theoretical results of the ARMOUR project;
• Showing real demos at important events to demonstrate reality of the solutions and interact with interested parties.

Exploitation-oriented phase

Finally, during the exploitation-oriented phase, specific activities will be undertaken in order to improve awareness on Security & Trust on the IoT. This dissemination phase is specifically targeted at potential users of the ARMOUR toolbox for enabling large-scale Internet-of-Things Security & Trust experiments, and also at interested parties on Secure & Trusted IoT applications certification. Specific activities of this phase include:

• Organisation of events such as workshop to build and disseminate project result potential;
• Publishing of the ARMOUR potential such as benchmark in order to increase appropriateness of the FIRE concept by the current research communities;
• Participation at important conferences and workshops, where the results of the project could be presented to stakeholders. Use demos to support contacts for future exploitation;
• Participation in conferences to show ARMOUR solutions such as Security & Trust related conferences;
• Participation in non-technical oriented conferences such as related to digital economy, users, and privacy to increase the awareness of ARMOUR solutions while preventing fears related to privacy.

1.4 Purpose of this deliverable

Dissemination activities are a core part of the ARMOUR’s community building plan, and essential for the achievement of results and impact of the ARMOUR programme. The objective of the ARMOUR dissemination strategy is to lay down the foundation for continuous communication, internally within the consortium, and externally, in respect to the stakeholders.

To achieve such impact, ARMOUR partners need to be effective and efficient in communicating a correct and aligned message to the outside world, based firmly on the substance, which was set out in the contracted DoA.

Therefore, ARMOUR need a set of Dissemination materials so to achieve external recognition in the community, and also to enable Stakeholders to be correctly informed and eventually become involved in participating activities relevant to their circumstances and needs. This Deliverable provides a detailed overview of the dissemination materials created for all ARMOUR’s outreaching activities and also provide a set of instructions on the best ways to customize the ARMOUR’s dissemination materials.

The project consortium has defined a set of dissemination instruments and materials to support the marketing, promotion and dissemination of ARMOUR. The main, include the project logo, project website, project flyers, a set of posters for widespread use.
2 ARMOUR: The brand

2.1 ARMOUR Logo

The ARMOUR project image was around five key topics from the project, that represents the values and the topics that ARMOUR addresses or relates to. These topics that supported the creation of ARMOUR image, are the following:

- Security / Protection
- Technology
- Confidence / Professionalism
- Electronic circuits
- Belonging to FIRE

Using the security / protection topic as inspiration, the main idea of the image is a shield. It's a very strong symbol that represents well the topic. Throughout history, even since medieval times, this symbol represents a weapon that protected us from all the attacks of enemies, protecting us of the attacks or ensuring that our advance on the enemy was effective. It has a great strength and it represents security well.

The technology and electronics are aligned at the same point. First, because we are talking about a project that is based on the discovery of new technological solutions for security tests. In turn, the electronics come from connections, data transmission in a network of virtual circuits.

Presenting a bold look, a strong image and a modern look, is achieved through the simplification of the shield, and the implementation of the above concepts in a balanced way. The icon of a shield has been modernized with the circuit lines, drawing a lock in the centre. The bold typography, was also inspired by the icon designed and chosen because of its resemblance to the icon (details of cuts in letters).

The last point, belonging to FIRE, was inspired for the colour of the icon for the logotype. It was a simple and tenuous gradient.
2.1.1 Logo Variants
There were made some versions of the logo to adapt better to various types of usage: posters, banners, cards, etc.

**Vertical version**

White Version  
Black Version  
Colour Version

**Horizontal version**

White Version  
Black Version  
Colour version

2.1.2 Protection areas of the ARMOUR logo
The area of protection of the logo ARMOUR is referenced by the thickness of the typography. It defines the edges for safety which must be placed, when used with other logos, being placed on the sides or above the right ARMOUR.

**Horizontal version**
2.2 Official colours

The colour of the ARMOUR Image was inspired in the FIRE logo, making the connection between the two. The logo conveys so one aspect of fire within the circuit, giving the illusion that is in constant motion, and with this concept, the notion that the armour is in constant evolution.

ARMOUR Logo

<table>
<thead>
<tr>
<th>Pantone P10-8U</th>
<th>Pantone P20-8U</th>
<th>Pantone P179-16U</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMKY</td>
<td>RGB</td>
<td>CMKY</td>
</tr>
<tr>
<td>C  0%</td>
<td>C 254</td>
<td>C 0%</td>
</tr>
<tr>
<td>M  0%</td>
<td>M 190</td>
<td>M 0%</td>
</tr>
<tr>
<td>Y  0%</td>
<td>Y 16</td>
<td>Y 0%</td>
</tr>
<tr>
<td>K  0%</td>
<td></td>
<td>K 0%</td>
</tr>
</tbody>
</table>

Layout Design

Main colours
### Secondary colours

<table>
<thead>
<tr>
<th></th>
<th>CMKY</th>
<th>RGB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMYK</td>
<td>C 0%</td>
<td>C 255</td>
</tr>
<tr>
<td></td>
<td>M 10%</td>
<td>M 222</td>
</tr>
<tr>
<td></td>
<td>Y 86%</td>
<td>Y 61</td>
</tr>
<tr>
<td></td>
<td>K 0%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CMKY</th>
<th>RGB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMYK</td>
<td>C 0%</td>
<td>C 247</td>
</tr>
<tr>
<td></td>
<td>M 50%</td>
<td>M 148</td>
</tr>
<tr>
<td></td>
<td>Y 100%</td>
<td>Y 61</td>
</tr>
<tr>
<td></td>
<td>K 0%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CMKY</th>
<th>RGB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMYK</td>
<td>C 0%</td>
<td>C 241</td>
</tr>
<tr>
<td></td>
<td>M 75%</td>
<td>M 101</td>
</tr>
<tr>
<td></td>
<td>Y 98%</td>
<td>Y 36</td>
</tr>
<tr>
<td></td>
<td>K 0%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CMKY</th>
<th>RGB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMYK</td>
<td>C 0%</td>
<td>C 194</td>
</tr>
<tr>
<td></td>
<td>M 0%</td>
<td>M 196</td>
</tr>
<tr>
<td></td>
<td>Y 0%</td>
<td>Y 180</td>
</tr>
<tr>
<td></td>
<td>K 27%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CMKY</th>
<th>RGB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMYK</td>
<td>C 0%</td>
<td>C 67</td>
</tr>
<tr>
<td></td>
<td>M 0%</td>
<td>M 67</td>
</tr>
<tr>
<td></td>
<td>Y 0%</td>
<td>Y 69</td>
</tr>
<tr>
<td></td>
<td>K 89%</td>
<td></td>
</tr>
</tbody>
</table>

### 2.3 Layout Design & Templates

The layout design was inspired in the electric circuit, with the lines and dots, connecting all the icons and text. The objective is to conduct the reading of the spectator and highlight the key information.

#### 2.3.1 Stationary

When the overall image for ARMOUR was chosen, it began the progress to create the final image of the layouts for the posters. This way, the concept to create the posters was divided in some areas to allow an easy construction of posters to disseminate the project.

The two big ideas to the general poster was to respect the two-dimensional design that was used in ARMOUR brand, and give it an edgy modern look. To pass these two ideas, it was chosen typography and iconography.

### Typography

The first concept using only typography there was made with a simple design, a catchy phrase that represented the brand. The lack of additional information of the project deliberately, the main idea was to stand out, make a difference, and capture the attention of the person that passed through them, gaining the curiosity to discover what the ARMOUR represent.

### Iconography

For this concept the main idea was, like in the concept above, catch the attention of the passing by people. Stand out of the "crowd". This time the main focus was the image in the centre, to transmit what ARMOUR did in a general idea. Additionally the content is displayed on the corners, to only give detail when the audience stands by close.

In this concept it was made a second poster, with some information displayed to the partner have an idea how the overall layout would look with all the information aspects and respecting the image created in this concept.
Contents

For the poster of contents, the area was divided in three. The black strip was the focus of the poster. It was made a clean layout so it can be displayed information in this area.
The Evolution of ARMOUR posters

Following this image, the three concepts written above (typography, iconography and content), were joined the best of the three ideas in one big concept: **Infographic posters**.

The infographic allows to not only want to make stand with the poster, but join the concepts of ARMOUR and the seven experiences to make a full, complete and appealing poster. The re-design of the layout allows to make a simpler construction, with defined areas. Also guides the reading of the observer with the dots, lines and arrows, giving the sense of movement.

This way there were made two templates for the general poster and the experiment poster like it can be seen below:

- The general poster is divided in 6 areas: Header, Highlight area, Information area, Details area, Website area, partners logos area.
- The experiment poster is divided in 7 areas: Header, Goal, Image, Security Threats/Details, Description, Legend, Website, Partners logos area.
For this layout were made new addition icons to make the graphics in the posters, with a two-dimensional aspect. It's also used the secondary colours defined in the Official Colours to give a significance to the graphic scheme (malicious/benign connections, entity, device, etc.).

**Layout construction for the two posters:**

**Layouts with information for the two posters:**
2.3.2 Website
For the website layout, the main idea was a clean and objective site, were the interface was simple to understand and use. The information was put in a concise way.

- Webpage template construction
The ARMOUR webpage template was design to look organized, clean and easy to use. It was divided in four distinct areas – Navigation Bar, Banner, Information and Footer.
• **Navigation bar**

The navigation bar provides a quick access to the different areas of the website. This element was thought to look easy, intuitive and in a smooth way so it doesn’t take the focus from the content.

• **Banner**

There were made several banners for the website. All the designs of the icons were inspired in the subject of the page where they are placed.

The banners were also thought to give a coherent look to the site, and to allow the user gets in a quick way where he is.

• **Information area**

Area reserved for the presentation of several kinds of contents related with the ARMOUR project.

The information is displayed in a clean and direct way, prioritizing the information, and this way, helping the user to organize his reading in the website. This information was disposed with highlight areas, light text (using bullets and a straight line of though), schemes, iconography and infographics. This way the it doesn’t turn heavy to the eye of the user, and quickly he gets the message.

For the interaction of the user in the website, it was though a simple way to change the information, so the user instinctively knows how it works.

We present below some examples of the website layouts to dispose information in this area.
This area was reserved to positioning the project inside the European Union's H2020 Programme. This way allows visitors to quickly identify that the work developed in this project is funded by the European Union.
2.3.3 Document Layout

Document Example

Lorem ipsum dolor sit amet, leo consectetur feugiat dui real, nibh odio vitae eleifend, mus magna

Call Identifier
H2020-ICT-2013

Project Reference
694237

Type of Action
RN - Research and Innovation

Start date of the project
09/2013

Duration
09/2016

Dissemination level
P: Public
C: Coordinator, only for members of the consortium (including the Commission)
D: Classified, information is not to be circulated outside of the Commission (Decision 2002/194/EC)

Abstract

Disclaimer
This document is produced. All activities, decisions and opinions expressed in this document are those of the authors, and do not necessarily reflect the official position of the European Commission. The Commission cannot be held responsible for any use that may be made of the information contained therein.
2.3.4 Slides Template

For the slides template, it was used a simple and clean design that maintains the design in the posters, and gives at the same time an edgy look. It was made with different areas – header, title, subtitle, the speaker, or information about the ARMOUR project, among others.
The inside layout was made as clean as possible to allow to put the information necessary without taking care about the bad reading with symbols that it wasn't necessary.

Cover Slide

![Cover Slide Image]

Internal Slide

![Internal Slide Image]
Subtitle Slide

Back cover #1: With fact sheet of the project
Back Cover #2 - Simple layout for message (Thanks, questions, etc.)
Presentation impact
2.3.5 ARMOUR Banner
For the printable banner to take to the expositions, it was given a strong and edgy look, that catches the attention of the people. The design follows the strong project image.

*How it would look in real world*
3 Dissemination Posters

Posters are intended to be presented on conferences, on public areas, where the message needs to be transferred fast, and make people easily aware of ARMOUR. Posters can be also used for aiding ARMOUR representatives in booths to explain in more detail what is ARMOUR, and for example, explain experiments in detail.

In the first period of the project, limited information about results is available, but dissemination being important, some strong image and material to support people to know the project is important.

Therefore, in the first period, support posters were focused in the available project content, mainly an overview poster about what is ARMOUR, and using the results of D1.1 - ARMOUR Experiments and Requirements, experiment posters based on the identified vulnerabilities were also produced.

During the rest of the duration of the project, additional posters will be made, representing the key results of the project.

Next, is presented the poster of ARMOUR overview and one specific for each experiment:

- Bootstrapping and Group Sharing;
- Sensor Node Code Hashing;
- Secured bootstrapping/join for the IoT;
- Secured OS / Over the air updates;
- Trust aware wireless sensor network;
- Secure service discovery;
- Secure IOT platforms.
3.1 What is ARMOUR?

**ARMOUR**

LARGE-SCALE EXPERIMENTS OF IOT SECURITY AND TRUST

**WHAT IS ARMOUR?**

Enhance outstanding FIRE IoT/Cloud testbeds with the ARMOUR experimentation toolbox for enabling large-scale Internet-of-Things Security & Trust experiments.

**TOOLBOX**

Enhance outstanding FIRE IoT/Cloud testbeds with the ARMOUR experimentation toolbox for enabling large-scale Internet-of-Things Security & Trust experiments.

**7 EXPERIMENTS**

Deliver a set of duly experimented and properly validated methods and technologies for enabling Security & Trust in large-scale Internet-of-Things conditions.

**CERTIFICATION**

Definition of frameworks to support the development of Secure & Trusted IoT applications and setting confidence on their deployment through benchmarking and a novel certification scheme.

---

Call Identifier: H2020-ICT-2015  
Topic: ICT-12-2015 Integrating  
Project Reference: 695217  
Type of Action: RIA - Research and Innovation action  
Start date of the project: February 15, 2016  
Duration: 24 months

[www.armour-project.eu](http://www.armour-project.eu)
3.2 ARMOUR Experiments

Bootstrapping and Group Sharing

GOAL

Define ways to allow devices to authenticate and request authorisation to publish information securely, as well as provide a communication mechanism for secure information exchange between groups of devices through the platform.

Security threats:
- Impersonation of legitimated devices by discovery of security elements
- Modification/replay of messages
- Unauthorized access to sensitive data

DESCRIPTION

1. A sensing device authenticates with the AAA Server and receives access to the network.
2. The sensing device requests a Token from the Capability Manager, which checks with the PDP if the device is authorised to publish on the IoT platform.
3. The sensing device publishes information to the Pub/Sub, attaching its capability token.
4. Information is forwarded to the devices that subscribed to the corresponding information topic. Data are secure exchange.
Sensor Node Code Hashing

**GOAL**

Maximisation of energy efficiency in security mechanisms based on code hashing techniques to prevent software to be acquired by 3rd party entities and devices to be programmed with illegitimate software.

**Security Threats**
- Intercepting it during a software update process and successfully read it
- Accessing a software update captured by a malicious device
- Extracting the software from a legitimate device

**DESCRIPTION**

Endpoint Devices - with very limited energy available and computation capabilities - request software updates

Software Provisioning Servers receive requests and start mutual authentication process based on hashing algorithms and software fingerprinting techniques

After successful authentication, software updates are sent to devices

Software executed in devices is highly optimised, where no generic Operating System is used and different software is deployed in devices with different purposes
Secured bootstrapping/join for the IoT
Secured OS / Over the air updates

Experiment Secured OS/ Over the air updates

Goal

The main objective of the experiment is to test, prototype and provide secured OTA (Over the air) updates for RIOT by testing various methods for distributing new software and configurations to devices.

Security threats
- Impersonating a Software Provider
- Injecting/Modifying Software Update
- Replaying Obsolete Software Updates
- Disrupting Software Updates

DESCRIPTION

The tested node receives a new firmware via its radio interface, over UDP and high-level encrypted channel.

The node stores the new firmware and checks the signature of this firmware.

The signature checks right.

The node boots the new firmware and verifies its functionality.

The new firmware functionality is confirmed to be correct.

The node has successfully updated its firmware.

www.armour-project.eu
Trust aware wireless sensor network

EXPERIMENT
TRUST AWARE
WIRELESS SENSOR NETWORK

GOAL
Evaluate the performance of distributed trust-aware WSN routing solutions in large-scale deployments and under the presence of malicious nodes.

Security Threats mitigated:
- Black-hole
- Grey-hole
- Replay of messages
- Modification of messages
- Man-in-the-middle attack

DESCRIPTION
Sensor nodes produce data that is forwarded to gateways using multi-hop routing algorithms.
Malicious entities are present in the network, executing different types of attacks.
Using the proposed RPL-based trust-aware solution, sensor nodes identify malicious nodes, adapting the routing algorithm to exclude them.
Multiple metrics can be composed and configured to allow the mitigation of several attacks.

The trust solutions under test are capable of tolerating several types of attacks while at the same time achieving optimal routing and satisfying application requirements.
Secure service discovery

GOAL

Execution of a set of experiments proving the robustness and efficiency of secure service discovery achieved by innovative solutions combining DTLS over CoAP protocol.

Security Threats

- Interception of keys exchanged between benevolent nodes communication
- Taking advantage of insecure cryptographic storage techniques
- Enforcing a software update process

DESCRIPTION

Sensing device, with constrained resources, register its services and resources onto the CoAP server

Sensing device exchanges security keys with the CoAP server and setup a secure communication channel

Network will be subject to different security attacks to test lightweight security solutions based on DTLS and CoAP protocols

Several encryption algorithms and integrity check methods will be used in this experiment
Secure IOT platforms

GOAL

Automation of security and exploratory testing addressing vulnerability issues on IOT platforms, aiming to the development of a methodology and approach to use Certiffy for standard compliance testing.

Security Threats
- Injections, for instance SQL injection, exploiting the vulnerabilities to gain unauthorized access
- Leaks or flaws in the authentication or session management functions to impersonate users

oneM2M
Platforms that adopted oneM2M standards for sharing M2M/IoT data among all applications

FIWARE
Platform providing public APIs to ease the development of Smart Applications

DESCRIPTION

1. Security Functional testing (co- agreed standard/specification): verifies if the system behavior complies with specification, allowing to detect possible security issues and if security functions are correctly implemented.

2. Vulnerability testing (Pattern driven): aims to identify and discover potential vulnerabilities based on risk and threat analysis by using security patterns as a starting point.

3. Security robustness testing (Behavioral Fuzzing): compute invalid messages sequences by generating weighted random test steps. It enables to tackle the unexpected behavior regarding the security of large and heterogeneous IoT systems.

www.armour-project.eu
4 Project Website

The ARMOUR project website is available on [http://www.armour-project.eu](http://www.armour-project.eu). The website contains all the necessary information regarding the project, its research and the goals set for the project. The website was created using WordPress, which is a very versatile content management system, commonly used worldwide. WordPress provided us with the flexibility to expose ARMOUR’s information using the concepts created for the project brand. So, the Website design is coherent with the Project Image already identified and explained in the previous chapter, and the current structure of the website is represented in following picture. It is important to note that this structure can suffer small changes during the execution of the project, due to possible enhancements that will reflect work under development.
Home

- Landing Page

![Landing Page](image)

Latest News

- [Landing Page](url)

Navigation Menu (Project)

![Navigation Menu (Project)](image)

Navigation Menu (Experiments)

![Navigation Menu (Experiments)](image)
Project

- **What is ARMOUR?**

The ARMOUR project aims to address Security and Trust issues in the Internet of Things by providing easy-to-implement and certified Security & Trust solutions for large-scale IoT systems. The project is funded by the European Commission under the Horizon 2020 program.

The Internet of Things (IoT) is rapidly growing, but security and trust are significant challenges. ARMOUR addresses these issues through a series of experiments and demonstrations in large-scale IoT environments. The project's goals include:

1. Establishing a platform for experimenting with IoT Security and Trust technologies.
2. Developing and testing new solutions for securing large-scale IoT systems.
3. Demonstrating the feasibility of implementing Security & Trust solutions in real-world scenarios.

ARMOUR's approach is to develop a toolbox of solutions that can be applied to different IoT environments. This toolbox includes:

- **Toolbox**

  - Upgrade FIRE testbeds for supporting large-scale IoT Security & Trust experiments.
  - Research and develop the ARMOUR technological experimentation suite for executing and managing Security & Trust experiments in large-scale IoT settings.
  - Create a prototype of the ARMOUR experimental infrastructure.
  - Enhance FIRE IoT systems to support real-world IoT experiments.
  - Develop a framework to support the design of Security & Trust experiments.
• **Experiments**

Provide experimented solutions for Secure & Trusted large-scale IoT environments

- Deliver certified procedures for large-scale Internet-of-Things security bootstrapping;
- Deliver certified mechanisms for large-scale trusted routing in Wireless Sensing Networks;
- Deliver demonstrated solutions for trusted service discovery in large-scale Internet-of-Things;
- Deliver attested schemes for sensors/devices code hashing in large-scale IoT environments;
- Deliver verified methods for secure Operating Systems in the large-scale Internet-of-Things;
- Deliver validated technologies for secure large-scale IoT systems integrated via FIWARE Clouds.

**Target Performance Indicators:**

- 7 (seven) different and much-relevant experiments of Security & Trust for large-scale IoT environments.

A set of 7 (seven) large-scale Internet-of-Things Security & Trust experiments have been defined that have been brought forward by the project partners based on their specific interests of technological performance improvement and/or innovation.

These experiments are concisely:

**Bootstrap and group sharing procedure**

A large-scale experiment on IoT security bootstrapping procedures, presented by CICAT, as to protect the access to services as a first step to enhance a holistic security approach for smart building scenarios.

**Sensor code hashing**

A large-scale experiment on sensor code hashing presented by EMPAeth to be used in their product line of trust anchors for providing secure and trusted monitoring services (especially of critical infrastructure).

**Secured bootstrapping/JOIN for the IoT**

An experiment aiming to testing protocols and provide secured communications to enable secured bootstrapping procedures while ensuring the establishment of standard and highly resilient communications.

**Secured OS I Over the air updates**

This experiment main objective is to test, prototype and provide secured OTA (Over the air) updates for RIOT, enabling the distributing new software and configuration of settings (e.g. credentials) to devices running RIOT while maintaining a high level of security.

**Trust aware wireless sensors networks routing**

A large-scale experiment on secure wireless sensor networks routing presented by Sensinode to enable their wireless sensor networks IoT solutions for large, scale conditions.

**Secure IoT Service Discovery**

A large-scale experiment on secure IoT service discovery presented by Sensinode to extend their field-proven products enabling secure and trusted monitoring services by remotely and geographically dispersed field nodes.

**Secure IoT platform**

An experiment on secure large-scale Internet-of-Things operation, using FIWARE Cloud technologies, presented by CICAT and DiSTeS with a specific interest of partners to take advantage of IoT using FIWARE technologies.

The ARMOuir experiments follow a well-defined methodology to ensure reproducible, extendable, applicable and reliable experiments. The ARMOuir experimentation methodology involves the following steps:

- Install and configure the scenario(s) for Internet-of-Things large-scale Security & Trust experimentation;
- Do the measurements and collect the experimentation data out of the ARMOuir experiments;
- Perform pre-processing (e.g. data cleaning) and organisation (e.g. transformations, semantic annotations) of the experimentation data;
- Analyze experimentation data (e.g. hypothesis) and perform benchmarking of experiments, compare performance of solutions;
- Report on the results of the experimentation (and possibly publish them for project dissemination).
- **Certification**

  Benchmarks, framework and certification for Secure & Trusted large-scale IoT.
  - Define a methodology for benchmarking Secure & Trusted large-scale IoT solutions and release benchmarks of the ARMOUR experiments and other relevant solutions for IoT Security & Trust;
  - Study how different security and privacy solutions or components, defined in their respective systems or contexts, can be used in a harmonised way to support the design and deployment of secure IoT applications;
  - Establish 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.

  Target Performance Indicators:
  - 1 (one) new benchmarking methodology and 1 benchmarks of large-scale IoT Security & Trust experiments;
  - 4 (four) relevant application domains of large-scale IoT studied and their Security & Privacy concerns analysed;
  - 1 (one) new labelling scheme for certifying large-scale IoT Security & Trust solutions and their applications.

- **Publications**
Experiments

- **Bootstrapping and Group Sharing**
Sensor Node Code Hashing
Secure Bootstrapping / Join for IoT
• Secure OS / Over the Air Update
• Trust Aware Wireless Sensor Network
Secure IoT Service Discovery
Secure IoT Platforms
The Consortium involves 8 partners from 5 European countries: France, Greece, Portugal, Spain and Italy.

ARMOUR is an SME-driven project: five (5 of 8) partners are high-tech SMEs (STN, SMA, UNPARALLEL, ESM, ODIN S) pushing experiments in Large-Scale IoT Security & Trust dimensions that are important to them as to improve their products/services, contributing to the exploitation of ARMOUR research solutions.

The academic (UPMC) and research institution (Inria) have a strong link to industry and various SMEs that are in their circle of influence and are informed about ARMOUR project. Its experiments and technologies. Notably, ARMOUR has the objective of creating a Large-Scale IoT Security & Trust enabling facility operated by Inria and supported by UPMC that is especially aimed at SMEs. JPC provides the essential research-based policy support to industry for a smooth large-scale IoT adoption.

**ROLE**


**EXPECTATION**


This project has received funding from the European Union’s H2020 Framework Programme for Research, Technological Development and Demonstration under grant agreement no 688257.
News

ARMOUR presented at ICT Week 2016 - Belgrade. Paolo Mancini (impresario) made a "More presentation of ARMOUR available in [ ]"

Kick-off Meeting

On 25th and 26th of February, the 8 partners of the ARMOUR consortium met in LYON (FR) for a premiss in Emirational...

Events

Coming Up

June 27 - June 30, 2016
European Conference on Networks and Communication, Greece

Past Events

May 31 - June 2, 2016
The Internet of Things Week 2016
Belgrade, Serbia
5 Flyer

Using ARMOUR Stationary it was also produced a Flyer to hand over to people, in order for them to capture the main idea of what is ARMOUR.
Flyer Detail #1

WHAT IS ARMOUR?

CONTACTS

PROJECT COORDINATION

P. S. Freitas
University Paris and Maine Cuba (UPMC)

DISSIMULATION COORDINATOR

Bruno Almeida
Université Paris-Sud
Eva de Barretó
Mariane Franque, Office 04

Tel:
+351 212.438.041

Email:
dissimation@armour-project.eu

LARGE-SCALE EXPERIMENTS
OF IOT SECURITY AND TRUST

Call Identifier
P.2004.47.2915

Type of Action
ICT - Research and
Innovation action

Topic
ICT-12.2015

Start date
February 9, 2016

Duration
24 months

Flyer Detail #2

TOOLBOX

Enhance outstanding FIRE IoT/Cloud testbeds with the ARMOUR experimentation toolbox for enabling large-scale Internet-of-Things Security & Trust experiments.

7 EXPERIMENTS

1. Secure bootstrapping and Group Sharing
2. Sensor Node Code Hashing
3. Secure bootstrapping/ join for the IoT
4. Secure OS / Over the air updates
5. Trust aware wireless sensor networks routing
6. Secure IoT Service Discovery
7. Secure IoT Platforms

CERTIFICATION

Definition of frameworks to support the development of Secure & Trusted IoT applications and setting confidence on their deployment through benchmarking and a novel certification scheme.
6 Conclusion

This Deliverable provided the already existing content for conducting the Project dissemination strategy. ARMOUR partners need to be effective and efficient in communicating a correct and aligned message to the outside world, based firmly on the substance, which was set out in the contracted DoA.

Therefore, a set of Dissemination materials was created to achieve external recognition in the community, and also to enable Stakeholders to be correctly informed and eventually become involved in participating activities relevant to their circumstances and needs. This Deliverable provided the dissemination materials already created for all ARMOUR’s outreaching activities and also provided a set of instructions on the best ways to customize the ARMOUR’s dissemination materials.

The dissemination materials created include the project logo, project website, project flyers and a set of posters for widespread use. However, there are some posters and flyers that were not yet created due to the project being in an earlier phase, such as posters regarding the ARMOUR Security toolbox or the ARMOUR certification and labelling framework, which are on an early stage and so will be created in a near future.
7 Bibliography

