PReparing Industry to
Privacy-by-design
by supporting its
Application in REsearch

Contribution to Study Periods Security Guidelines for the Iot and Privacy Guidelines for the IoT

Security and Privacy from an Interoperability Perspective

Version: v1.0
Date: 10/3/2017
Confidentiality: Public

Author/s: Antonio Kung (Trialog)

PRIPARE has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no ICT-610613

CREATE-IOT has received funding from the European Union's H2020-EU.2.1.1. - INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)
under grant agreement no ICT-732929

Table of Contents

Document History

Version	Status	Date
V0.1	Initial version of the Table of contents	01/03/2017
V1.0	First version	12/03/2017

Author		
	Name	**Date**
	Antonio Kung	12/03/2017

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
API	Application Programming Interface
EIP-AHA	European Innovation Platform on Active Healthy Ageing
EIP-SCC	European Innovation Platform on Smart Cities and Communities
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOT	Internet Of Things
ISO	International Organization for Standardization
LSP	Large Scale Pilots
NIST	National Institute of Standards and Technology
PI	Point of Interoperability
PPI	Pivotal Points of Interoperability
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch
SLA	Service Level Agreement
W3C	World Wide Web Consortium

Table 1: Acronym table

Executive Summary

This document provides an analysis on how different viewpoints on the Internet of Things can influence the structure for security and/or privacy guidelines in the IoT.

The following viewpoints are presented:

- an IoT reference model viewpoint,
- an IoT abstract model viewpoint,
- a platform viewpoint
- an interoperability viewpoint
- a stakeholder viewpoint

It then shows how security and privacy concerns can be addressed taking into account the previous viewpoints, in particular the interoperability viewpoint.

It concludes with the recommendation to work on a future common new work item proposal: *Guidelines for security and privacy in a common IoT interoperability framework*

1 Introduction

The PRIPARE initiative was established in 2013 to coordinate work in Europe concerning privacy engineering. PRIPARE established a liaison with ISO/IEC JTC1/SC27/WG5 in October 2014 and has since being active in contributing in the area.

PRIPARE has also joined a number of initiatives related to the Internet of Things. It is now a member of Create-IoT[1], a 3-year support action that started in January 2017. The objective of Create-IoT is the following:

> Create-IoT's aim is to stimulate collaboration between IoT initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms. It requires cross fertilisation of the various IoT Large Scale Pilots (LSPs) for technological and validation issues of common interest across the various application domains and use cases. Create-IoT will align the activities with the Alliance for Internet of Things Innovation (AIOTI) and will coordinate and support the upcoming LSPs in sustaining the ecosystems developed during those projects through mapping the pilot architecture approaches, address ***interoperability and standards approaches at technical and semantic levels for object connectivity, protocols, data formats, privacy, security, trusted IoT, open APIs and share the road-mapping with international initiatives***.

Create-IoT has links with a number of initiatives and projects:

- The alliance for the Internet of things Innovation private-public partnership (AIOTI)[2].
- The ACTIVAGE large scale pilot[3], a 42-month €25 million undertaking started on January 1st, 2017 for the deployment and operation at large scale of Active & Healthy Ageing IoT based solutions and services.
- The SYNCHRONICITY large scale pilot[4], a 34-month €20 million undertaking started on January 1st, 2017 for the delivery a harmonized ecosystem for IoT-enabled smart city solutions.
- The IOF2020 (Internet of Food and Farm 2020) large scale pilot[5], a 48-month €37.7 million undertaking started on January 1st, 2017 for the demonstration of innovative IoT solutions for a large number of application areas. It will involve IoT integrators and end users from the Arable, Dairy, Fruits, Vegetables and Meat verticals. There will be 5 trials covering 19 use cases.
- The AUTOPILOT large scale pilot[6], a 36-month €25.4 million undertaking started on January 1st, 2017 for the bringing of IoT into the automotive world to transform connected vehicles into highly and fully automated vehicles.
- The MONICA large scale pilot[7], a 36-month €17.6 million undertaking started on January 1st, 2017 for the demonstration of innovative wearable and portable IoT sensors and actuators to offer a multitude of simultaneous, targeted applications..

[1] http://cordis.europa.eu/project/rcn/206371_en.html
[2] http://www.aioti.org/
[3] http://cordis.europa.eu/project/rcn/206513_en.html
[4] http://cordis.europa.eu/project/rcn/206511_en.html
[5] http://cordis.europa.eu/project/rcn/206761_en.html
[6] http://cordis.europa.eu/project/rcn/206508_en.html

This report provides an analysis on how interoperability considerations change requirements on transversal concerns such as security and privacy, Further work taking this report conclusions could lead to useful contribution at standardisation level.

[7] http://cordis.europa.eu/project/rcn/206397_en.html

2 Viewpoints on the Internet of Things

It is useful to provide a number of high-level views of an internet of thing environment.

2.1 A Reference Model Viewpoint

Figure 1 is a typical IoT reference model[8]. It includes 4 horizontal layers and two vertical layers.

- the four horizontal layers focus on the interactions between applications and things. They include
  - the application layer, where IoT applications are running
  - an application support layer, which provide overall system capabilities to IoT applications
  - the network layer which provides transport capability
  - the device layer which provides device access capability
- the two vertical layers focus on transversal aspects of the whole system. They include
  - management capability
  - security concerns .

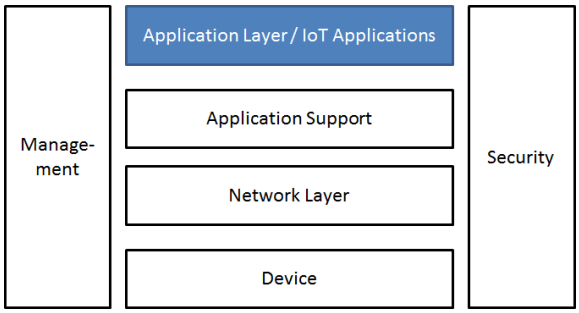

Figure 1: Reference Model View

The IoT reference model is useful in an IoT framework document to map the various subsystems making up an IoT system.

2.2 An Abstract Model Viewpoint

Figure 2 shows a simple abstract model of the Internet of things: IoT applications interact with things.

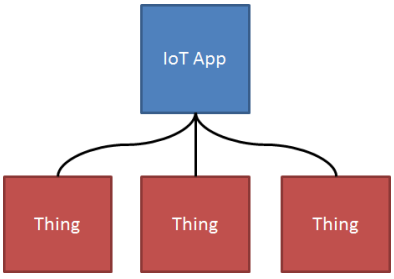

Figure 2: Abstract View

[8] It is directly inspired from the IoT reference model described in the ITU overview document on the internet of things [1].

This view captures the essence of the IoT, i.e. IoT applications take advantage of capabilities provided by things[9].

2.3 A Platform Viewpoint

Figure 3 shows a platform view of IoT systems. In this view, IoT applications run on top of platforms. In practice a platform provides to an Application an API or application programming interface. The figure assumes a unifying platform used as the glue for other platforms, recognizing the fact that several platforms could be involved[10].

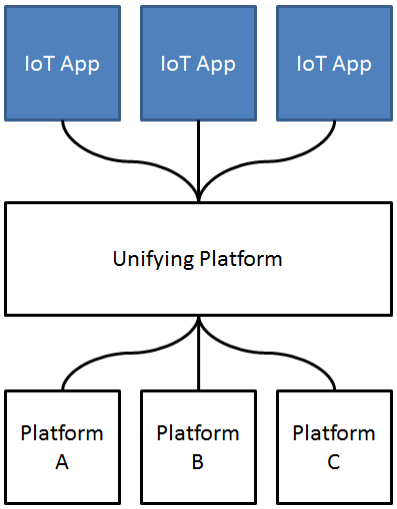

Figure 3: Platform View

The platform view is the most operational view for IoT application developers. It also provides an indication that the most prominent standardisation needs perhaps resides on the interfaces between applications and the underlying platform (s).

2.4 An Interoperability Viewpoint

As defined in [4], *Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the customers*.

Figure 4 provides an interoperability viewpoint model. It shows two types of artefacts: subsystems and points of interoperability (PIs)[11]. Figure 4 also shows that interoperability is a transversal concern: points of interoperability might be as different levels, i.e. a subsystem might also include subsystems and further PIs[12].

[9] This view has been used in the W3C web of thing initiative [2].
[10] The W3C initiative has assumed this view [2]. The C2 action of the European Innovation Platform on Active Healthy Ageing [4] pointed out in its recommendation O4 the need to reuse features from different platforms (for instance FIWARE - https://www.fiware.org/foundation or universAAL - https://www.fiware.org/foundation)
[11] Point of interoperability is a term used in the NIST International Technical Working Group on IoT-Enabled Smart City Framework [3]
[12] Such aspects are in general best captured through a layered based approach, for instance a reference model approach. [4] describes for instance an interoperability framework integrating the following layers: legal and regulatory, policy, process, information, application, IT infrastructure.

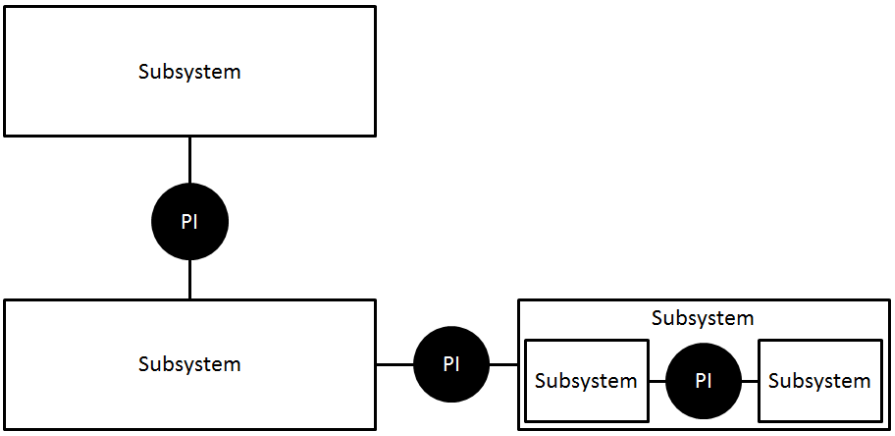

Figure 4: Interoperability Viewpoint

Figure 5 shows the relationship between the abstract viewpoint and the interoperability viewpoint. In this view, one single point of interoperability is highlighted, the one which connects IoT applications with Things. Since semantic interoperability is the main focus at an abstract level, we have called this PI the *IoT semantic interoperability PI*.

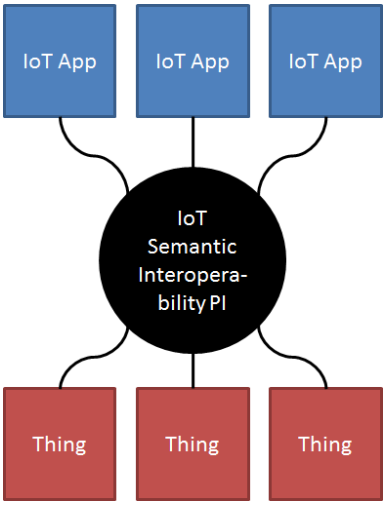

Figure 5: Interoperability in Abstract Viewpoint

Figure 6 shows an alternative interoperability model focusing on platform. Two points of interoperability are displayed:

- The IoT Semantic Interoperability PI
- A Platform Interoperability PI[13].

The two points of interoperability are probably the two most important points of interoperability in an IoT system[14]

[13] The concept of platform interoperability has been extensively discussed in EIP-AHA. See [4][5][6][7]
[14] Using terminology proposed by the NIST International Technical Working Group on IoT-Enabled Smart City Framework [3], we believe that they are the top two pivotal points of interoperability (PPI).

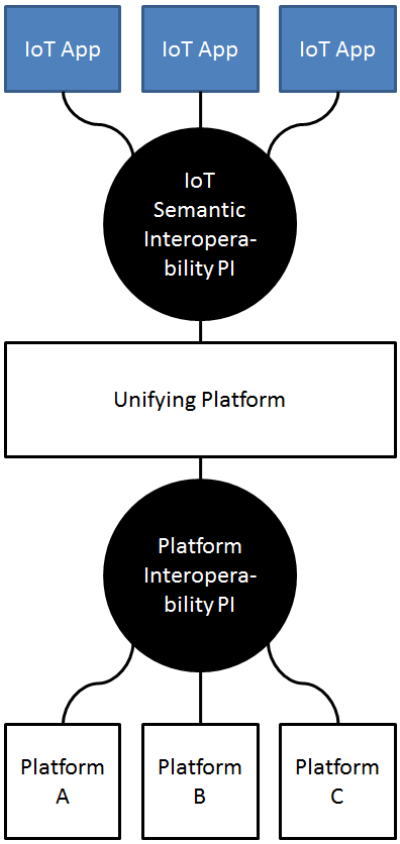

Figure 6: Semantic Interoperability and Platform Interoperability

2.5 A Stakeholder Viewpoint

Figure 7 provides a stakeholder viewpoint example. It describes the relationships between

- Stakeholders (e.g. user, IoT App supplier, IoT platform supplier, IoT App operator, IoT platform operator)
- Phases in the IoT system life cycle (e.g. design, procurement, deployment)
- Objectives and concerns targeted by the IoT system (e.g. IoT function, security, privacy, safety)

The relations are the following

- The lifecycle phases address the objectives and concernts targeted by the IoT system
- In the design phase, IoT application designers interact with users in order to apply a human centric design process (the co-creation process)
- In the procurement phase, the IoT system is built up. It involves IoT application suppliers as well as IoT platform suppliers.
- In the deployment phase, operators are involved. The figure shows two possible operators, the IoT application operator and the platform operator[15].

[15] This vision is increasingly adopted. One example of initiative is the EIP-SCC urban platform initiative: https://eu-smartcities.eu/content/urban-platforms

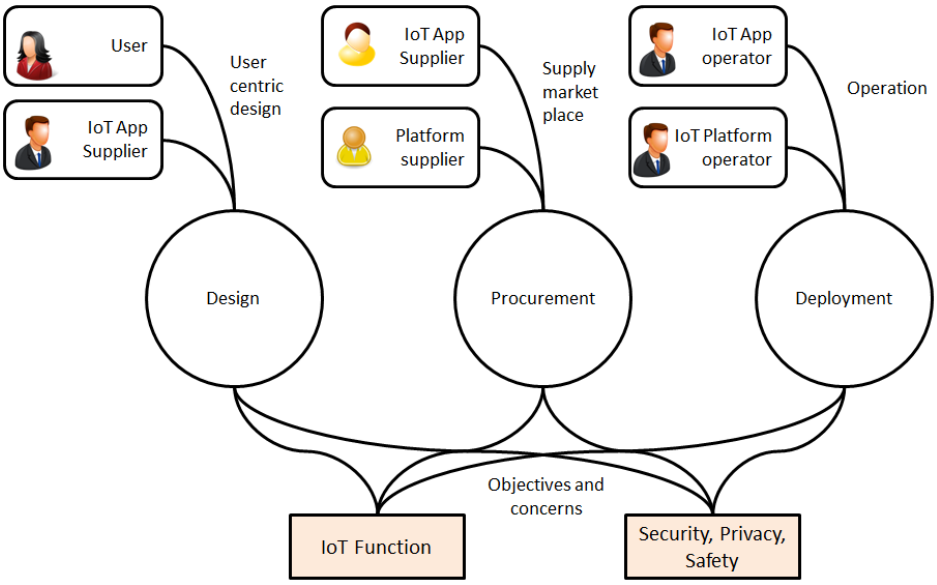

Figure 7: Stakeholder Viewpoint

Figure 8 shows the viewpoint combining stakeholders, phases, objectives and concerns and the abstract model. The resulting viewpoint points out the following:

- The objective and concern at design time must be considered at IoT application level, at semantic interoperability level and at the thing level.

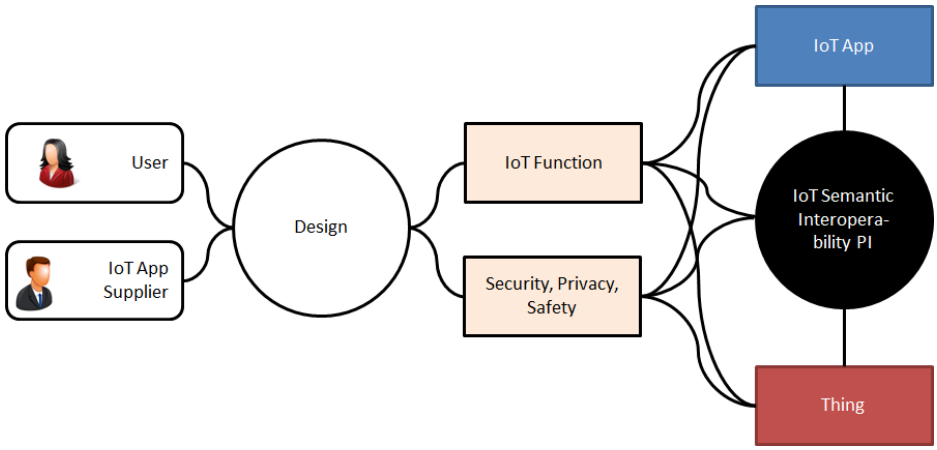

Figure 8: Stakeholder and Interoperability Viewpoint

3 Security and Privacy using Previous Viewpoints

Figure 9 shows how security and privacy can be addressed from an interoperability perspective in the IoT:

- An IoT application security and privacy-by-design approach must be used.
- It relies on security and privacy service descriptions that are associated with IoT semantic interoperability specifications
- These descriptions rely on features provided by the things which have been developed through a thing security and privacy-by-design process

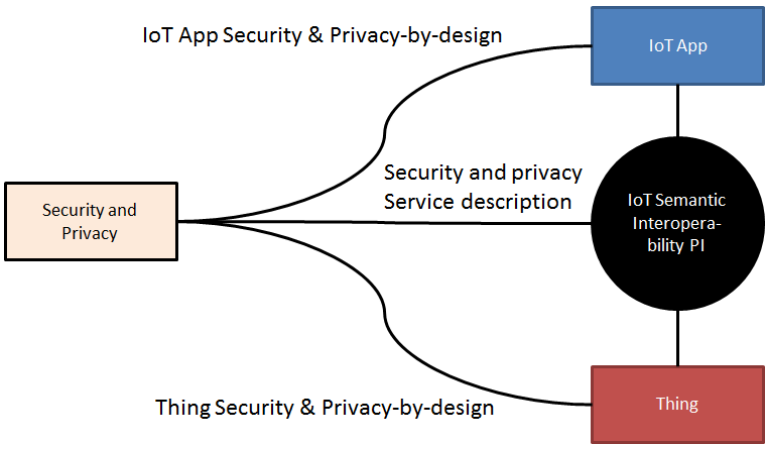

Figure 9: Security and Privacy from an Interoperability Perspective

Figure 10 shows the same viewpoint when platforms are taken into account. In this approach,

- the *thing* is replaced by an unifying platform, a platform interoperability PI and a number of platforms
- the *thing security&privacy-by-design* is replaced by platforms security-and-privacy.

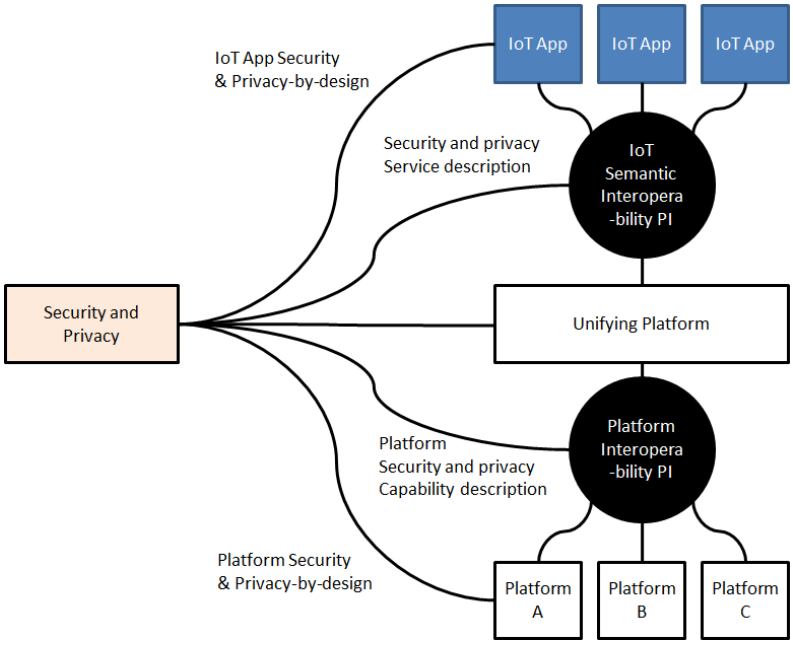

Figure 10: Security and Privacy from an Interoperability Perspective Integrating Platforms

4 Proposal for Further Work for ISO/JTC1 SC27

This contribution shows that guidelines on security and privacy for the IoT could be more effective if they are well integrated with guidelines concerning other concerns.

We showed that the following models: reference model viewpoint, abstract model viewpoint, platform viewpoint, interoperability viewpoint, and stakeholder viewpoint can have an influence on how the guidelines should be structured. From the previous sections, the guidelines would consist of

- *guidelines for IoT application security and privacy-by-design*,
- *framework for security and privacy service descriptions* that are associated with IoT semantic interoperability specifications,
- *guidelines for thing security and privacy-by-design*. If a platform viewpoint is further taken, this part could itself be structured as follows:
    - requirements for unifying platform security and privacy capability,
    - guidelines on platform security and privacy capability description,
    - guidelines for platform security and privacy-by-design.

We suggest that both the security and privacy study periods work on a future common new work item proposal: *Guidelines for security and privacy in a common IoT interoperability framework*.

5 References

[1] ITU-T Y.2060 Next Generation Networks – Frameworks and functional architecture models. Overview of the Internet of things. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items

[2] White paper for the web of things. http://w3c.github.io/wot/charters/wot-white-paper-2016.html Also see web of things Working group. https://www.w3.org/WoT/WG/

[3] International Technical Working Group on IoT-Enabled Smart City Framework. See https://pages.nist.gov/smartcitiesarchitecture/ and https://pages.nist.gov/smartcitiesarchitecture/community/consensusppi/

[4] March 2015 - C2 recommendation report. See https://ec.europa.eu/eip/ageing/actiongroup/index/c2_en and https://ec.europa.eu/eip/ageing/sites/eipaha/files/library/54f60825ddcca_interoperability.pdf

[5] March 2015 - EIP-AHA Summit. Brussels. https://ec.europa.eu/research/innovation-union/pdf/active-healthy-ageing/summary_wsg.pdf

[6] May 2015 - eHealth Riga. https://www.eiseverywhere.com/file_uploads/f41398f4a4d1809e58b12ee18770990d_AntonioKungRapporteur.pdf

[7] September 2015 - AAL Forum Ghent. http://fr.slideshare.net/AALForum/eipaha-towards-platform-interoperability

[8] Urban platform initiative of the European Innovation Platform on Smart Cities and Communities. https://eu-smartcities.eu/content/urban-platforms