Title of the article

Mahieddine Yaker
and Julien Cartigny
and Gilles Grimaud
IRCICA
University of Lille
address in Lille
Email: yyy@yyy.com

Chrystel Gaber
and Xiao Han
Orange Labs,
Châtillon, France
Email: firstname.lastname@orange.com

***Abstract*—Abstract**
TBD

I. Introduction

Introduction to be written.
TBD

mds
March 05, 2018

II. Isolation model

Part for Lille
Lille

III. Industrial ecosystem

This section aims at identifying and defining stakeholders involved in the use and management of an IOT or M2M device. The responsibilities of each actor are then described. In this section, we consider that a domain is an isolated area which belongs to an entity. The notion of domain is further precised in section IV-A.

A. Actors

We identify 6 stakeholders, namely the manufacturer, maintainer, owner, administrator, service provider and user, which interact with the IOT ot M2M device.

1) Manufacturer: It issues the device and the isolation solution. It also provides each device an identifier that will subsequently allow it to be identified as well as intial secrets that will allow the owner to access the device. It may also provide the drivers and software components for the sensors or actuators on the device.

2) Maintainer: It maintains the device, monitors the hardware components status and applies the patches deliveres by the manufacturer. This role can either be assumed or delegated to a third party by the manufacturer.

3) Owner: The device belongs to the Owner who defines an access policy to authorize which other entities are authorized to use or manage the device or domains within the device. The Owner can possess several devices. It receives initial credentials from the manufacturer that allows it to access each device in his fleet.

4) Administrator: It enforces the policy defined by the owner for his fleet of devices. If any modification, such as adding a new entity or modifying its granted permissions, is required, it requests a decision from the owner. This role can either be assumed or delegated to a third party by the owner.

5) Service Provider: It delivers a user-friedly service on one or multiple devices using the ressources authorized by the Owner. It installs or activates a service within the device. Muliple Service Providers can co-exist on the same device.

6) User: Users consume the services provided by the entities mentioned above. We can distinguish platform users and technical users. Service users subscribe to the services provided by the Service Providers. Technical users are typically members of the Owner, Manufacturer, Maintainer entities and they will perform authorized administration actions such as creating a new domain, granting rights to a new user, loading a service on the device. In the rest of this article we focus on platform users.

B. Responsibilities model

The responsibilities described in this section are described in table I.

The manufacturer provides the mechanisms and temporary credentials to personalize the device. At delivery, it provides the keys of the owner domain. The manufacturer is responsible for providing drivers which are compatible with virtualization and usage by multiple entities. For example, to control the position of an armed robot, it is better to literally express the coordinates of the destination. The command ”go to (x=10;y=40;z=20)” leads to less confusion than ”go to current position + (x=10; y=20; z=30). The manufacturer provides a platform in a safe state to the owner and does not keep any access to the manufacturer domain. In particular, the manufacturer does not manage access control to the drivers.

The Owner finalizes the personalization of the device after delivery by the manufacturer. In particular, the owner should modify its temporary credentials. Owner authorizes the usage of the device resources. If some resources are very sensitive, he provides the access to them through the use of a token which he delivers and verifies. The owner can choose that

some resources are accessible freely without the use of a token and thus reducing the security. The owner must not have any control or visibility on the actions performed by other entities unless it touches sensitive functions which the owner has decided to control through token verification.

If the owner delegates his tasks to an administrator, then the administrator can configure which resources need to be accessed with a token and the administrator is responsible for verifying the token and should not be able to control or visualize the actions performed by other actors unless they concern his perimeter of action.

The maintainer keeps the firmware, driver or any software in his perimeter up to date. This responsibility is key in the future as the regulators start to take actions on this point. For instance, the European Commission's overall security strategy [1] requires vendors to the commit to update their software in the event of newly disclosed vulnerabilities, as part of "duty of care" principle. Such initiative also exists in the United States with the Internet Of Things (IoT) Cybersecurity Improvement Act of 2017 [2].

Any entity which owns a partition (administrator, service provider, and maintainer) has to authenticate the machine (or user) who is sending the commands to the partition. This entity can choose to not perform and access control verification, thus reducing the security of the system. Any entity which owns a partition (administrator, service provider, and maintainer) is responsible for modifying the temporary credentials of its associated domains.

C. Architecture requirements

1) Domain isolation:

2) Owner non-interference: In particular, the owner or the administrator who have access to a privileged domain must not have any control or visibility on the actions performed by other entities if these actions do not involve device ressources which are under the responsibility of the owner.

3) Ressource access control: A device ressource access policy under the control of the owner or the administrator is mandatory. For each domain, a domain ressource access policy under the control of the domain owner (maintainer, service provider) is optional.

TBD

IV. Architecture & Security model proposed

To be done by Orange & Lille

A. Definition of a domain

B. Components of a domain

1) Configuration Manager: The Configuration Manager can be divided into two functions and sub-components, the isolation manager and the internal communication manager. The isolation manager provides the tools to create, read, modify or delete a domain. This module also contains a security policy which indicates which tasks and partitions should be started when the domain is started. This security policy also creates the communication channels between the tasks and partitions in the domain. The internal communication manager is the unique entry point of the domain.

2) Virtual sensors or actuators: The drivers are provided by the manufacturer of the device and are stored in a separate domain. Each domain contains a virtual sensor or actuator which exposes the functions of the actual sensor or actuator and acts as an interface with it. This allows the entity which owns the domain to see his domain as an actual device without knowledge of the isolation. The instruction and response are transmitted to and from the real driver using the internal communication mechanism.

3) Administration Manager: This module exposes the domain's ressources to an external server managed by the entity which owns the domain. It routes the command to read, write, execute the ressource to the expected manager or virtual sensor, actuator. It sends each command received to the Token & Security Validator.

4) Token & Security Validator:

5) Key Vault: This module stores the keys that are used by the domain. In particular, the keys used by the Token & Security Valdiator are stored here. It also provides the functions to add a new key, modify or delete an existing key.

C. Communication model

Section to be completed by Lille

Lille

D. Management model

V. Evaluation

section to show how the isolation model allows to address th industrial needs TBD

VI. Conclusion

The conclusion goes here.

Next steps : implementation and performance evaluation

Acknowledgment

This article was done in the scope of the European Celtic-Plus project ODSI.

References

[1] ENISA. Baseline security recommendations for iot in the context of critical information infrastructures. Technical report, ENISA, 2017.

[2] Mark Warner, Gardner, Wyden, and Senate of the United States Daines. Internet of things (iot) cybersecurity improvement act of 2017. https://www.congress.gov/115/bills/s1691/BILLS-115s1691is.pdf, August 2017.

TABLE I
RESPONSIBILITIES MATRIX

Requirements	Manufacturer	Maintainer	Owner	Administrator	Service Provider
Provide mechanisms & temporary credentials for initial device personalization before delivery to the owner	X				
Provide drivers compatible with virtualization & multi-tenant usage	X				
Provide temporary credentials for initial domain personalization to entities after delivery to the owner			X	X	
Update regularly the credentials to access the domain under its responsibility	X	X	X	X	X
Provide the device to owner without a remote backdoor access	X				
Create / Modify / Delete a domain before delivery to owner	X				
Create / Modify / Delete a domain after delivery to owner			X	X	
Configure the access policy of the device ressources			X		
Enforce the device ressource access policy			X	X	
Configure the domain ressource access policy	X	X	X	X	X
Enforce the domain ressource access policy	X	X	X	X	X
Keep the firmware & drivers up to date	X	X			
Keep the service applications up to date					X