H2020 Work Programme 2016-2017
H202-IoT-02-2016
Duration: 36 months

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 01.08

Coordination Event: Common event with the IoT projects addressing security for supporting the common activities

Revision: 1.0
Due date: 30-11-2018 (m23)
Actual submission date: 09-11-2018
Lead partner: SINTEF

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D01.08 Coordination Event: Common event with the IoT projects addressing security for supporting the common activities.**				
Status	< Released>	**Due**	m23	**Date**	30-11-2018
Author(s)	O. Vermesan (SINTEF), R. Bahr (SINTEF), R. Armitt Little (ATOS), P. Annicchino (AS), Dimitra Stefanatou (AL)				
Editor	O. Vermesan (SINTEF)				
DoW	This deliverable summarizes part of the work carried out in task T01.01 (IoT Focus Area coordination and road mapping) and includes a short summary of the IoT security and privacy workshop carried out 30th October 2018 in Brussels. This was a common event with the IoT projects addressing security for supporting the common activities. The meeting was organised to offer the basis for interaction and then built up the relations with different projects that have complementary activities. The goal was bringing the communities together and develop further the relationships based on the common needs and interests.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	19-10-2018	SINTEF	Template/Initial version.
0.01	15-10-2018	SINTEF	Workshop 30.10.2018 agenda.
0.02	06-11-2018	SINTEF	Document structure and general information.
0.03	07-11-2018	SINTEF, ATOS, AS	Workshop summary.
0.05	12-11-2018	SINTEF, AS	Review.
0.09	14-11-2018	SINTEF	Review comments considered.
1.00	14-11-2018	SINTEF	Final version released.

Table of contents

1. EXECUTIVE SUMMARY

1.1 Publishable summary

The Internet of Things security and privacy workshop was carried out 30th October 2018 in Avenue Beaulieu 25, Brussels. This was a common event with the IoT projects addressing security for supporting the common activities. The meeting was organised to offer the basis for interaction and then built up the relations with different projects that have complementary activities. The goal was bringing the communities together and develop further the relationships based on the common needs and interests.

1.2 Non-publishable information

None, the document is public.

2. INTRODUCTION

2.1 Purpose and target group

This was a common event with the IoT projects addressing security for supporting the common activities. The meeting was organised to offer the basis for interaction and then built up the relations with different projects that have complementary activities. The goal was bringing the communities together and develop further the relationships based on the common needs and interests.

2.2 Contributions of partners

SINTEF contributed to the organization of the event, the content of all sections of the document and provided a presentation and actively participating at the discussions during the event.
ATOS has contributed to the discussion and provided inputs to section 4.1.
AS contributed to the organization of the event and a presentation during the event.
AL contributed with a presentation during the event and by providing input under Chapter 2 and 3 of this report.
ETSI contributed with a presentation during the event.
TL contributed with a presentation during the event.

2.3 Relations to other activities in the project

This event was organized within the framework of activities of CREATE-IoT project falling under WP01 on Coordination and Support to the IoT Focus Area. The content of the workshop is closely linked to the work performed under WP05 of CREATE-IoT focusing on IoT Policy Framework - Trusted, Safe and Legal Environment for IoT. The workshop was, also, relevant for the scope of Activity Group AG05 covering privacy and end-user engagement.

3. WORKSHOP SUMMARY

Bellow we give a short summary of the IoT security and privacy workshop which took place in Avenue Beaulieu 25, Brussels 30th October 2018. It is organized around bullet points which underline the main points of each presentations. The slides of the presentations, with all the details, are available in the CREATE-IoT and IoT European Large-Scale Pilots Programme eRooms.

Figure 1: A snapshot from the IoT security and privacy workshop event

3.1 Morning session

3.1.1 The IoT European Large-Scale Pilots Programme (CREATE-IoT)

- Overview LSPs use cases
- Security/trust/ components
- Links with 3D reference architecture (by design)
- Example from Autonomous vehicles
- Question on what will be shared from AUTOPILOT?
  - Answer is that most deliverables are public and will be shared

3.1.2 Blockchain/DLT (CHARIOT)

- Blockchain based PKI system
- Interledger IoT system federation
- Smart contracts vulnerable if BC not reliable, contracts are not static
- BC is not GDPR compliant

- Cluster workshop on blockchain April 2019 (IBM Ireland)

3.1.3 Standards for lifecycle management of security and trust (IoTCrawler)

- IoT lifecycle management
- Document is under preparation, building on/linking to other initiatives (remind contributions)
- IoT needs a life-cycle approach
- Find gaps in current standards baseline
- Develop methodology
- Use security system framework (such as the NIST Framework)
- How to feed ETSI and ISO work, find multipliers?

3.1.4 AAA layer for end-to-end security with heterogeneous IoT devices (BRAIN-IoT)

- Converge on a common methodology for risk assessment and threat analysis
- Invite other projects to join + ETSI
- Devices + platforms
- Need to add privacy perspectives
- Include severity (outputs)
- Issues
  - End to end (need to know principle)
  - Secure storage of confidential info
  - Limit impact of security
  - Secure enrolment and bootstrapping (integrate oneM2M approach)
- Links with Ref architecture to be strengthened

3.1.5 Tools and approaches for dynamic screening of security and trust parameters (ENACT)

- Repository of tools and approaches for DevOps for IoT systems
- Initial structure being defined
- Guidelines on how to publish tools in the repository
- Use NIST cybersecurity framework as index
- Open for suggestions, feedback
- Want to start populating the repository
- Workshop in IoT Week
- Contribute to ISO work
- Create IoT could contribute to this

3.1.6 Discussions (morning session)

- What about end of life decommissioning?
- Need for open lifecycle management for security etc.

3.2 Afternoon session

3.2.1 End-to-end Security and Privacy by Design for AHA-IoT Applications and Services (ACTIVAGE)

- Problems in getting realistic risk assessment
- GDPR difficult to understand
- Useful experience to be shared if possible, on use case risk assessment and GDPR compliance

3.2.2 IoT Platform Interoperability (InterIoT, IoT-EPI)

- Have developed a set of building blocks for inter platform implementation + data semantics

3.2.3 IoT Policy and Legal Frameworks Overview (CREATE-IoT)

- Trust is a key asset
- Focus on non-functional aspects
- Need for an organisational framework in addition to technology and code of conduct
- Necessity to go beyond tick the box compliance towards accountability: the appropriate level of compliance in a particular situation; dynamic, principle-based, risk-based and impact-based. Accountability is also the main, dynamic notion to meet in the GDPR.
- New webinars, surety/privacy/trust in application contexts
  - Personal wearables, moving sensors, long-term fixed IoT Applications

First webinar of the new series will be on 9 January 2018 at 10.00 CET, about Wearables.

3.2.4 ISO Activities on IoT Security Standardisation (CREATE-IoT)

- Easy to contribute to ISO/IEC
- Identify strategic standards which are relevant and generate momentum

3.2.5 GDPR activities IoT-LSPs Programme & Privacy and End-user Engagement (CREATE-IoT)

- AG5 survey on privacy of LSPs
- Need for further feedback from LSPs on GDPR if possible
- Data ethics survey under way

3.2.6 IoT Security, Privacy, Interoperability Activities (CREATE-IoT)

- TC CYBER, TC SmartM2M STF 547
- STF 547 security/privacy of IoT platforms, Smart M2M work programme
- LSP use cases could be used for security/privacy

3.2.7 Discussions and follow-up (afternoon session)

- Identify gaps in lifecycle management standards (IoTCrawler)
- Identify further blockchain/DLT use cases, explore contributions to wider EU BC activities (CHARIOT)
- Start populating the IoT lifecycle management tools repository (ENACT)
  - Workshop in IoT Week
  - Contribute to ISO work
- Useful experience to be shared if possible, on use case risk assessment and GDPR compliance (ACTIVAGE + LSPs)
- LSP use cases could be used for security/privacy (ETSI, ETSI security Week)
- How to promote the value of standards and guidelines
- Free flow of data, NIS directive to be further explored
- Agree on how to share workshop information, AIOTI

It should be stressed that the set of common events of CREATE-IoT project and IoT European Large-Scale Pilots Programme planned in the course of 2019 in the context of WP05 IoT Policy Framework - Trusted, Safe and Legal Environment for IoT could, also, be considered as follow-up actions linked to the topic of the workshop addressed by the present report. In particular, building on the respective deliverable produced in 2017, D05.07 Legal IoT Framework Common Event scheduled for June 2019 will essentially stimulate discussions around NIS Directive, GDPR, the Free Flow of Non-Personal Data and the status of the Cybersecurity Act that from the point of view of security are of relevance for all the project participating in the earlier stated

cluster. In addition, on the basis of the respective deliverable document, also, submitted in 2017, WP05 of CREATE-IoT Project provides for D05.08 IoT Policy Framework Common Event with the IoT LSPs at aligning the IoT Policy Framework originally proposed and discussing recommendations in view of producing the final version. Notably, security and trust that were extensively discussed in the workshop summarized in the present report, form together with privacy and engagement the key pillars of the IoT Policy Framework introduced by CREATE-IoT Project.

Moreover, the upcoming set of application centric webinars mentioned under section 3.2.3 of the present report organized under the auspices of WP05 of CREATE-IoT Project in 2019 are of open attendance and, therefore, open to the projects of the IoT Cluster. It is expected that these webinars will strengthen cross-fertilization and pave the ground for the forthcoming common events.

A follow-up activity is including in the agenda of D01.09 Public-Private Partnerships collaborative event an overview of the areas of focus of the IoT Cluster projects (blockchain, IoT lifecycle management, risk assessment tools etc.) so to raise discussion and align with the activities of different.

4. CONCLUSIONS

4.1 Contribution to overall picture

The document includes the inputs collected from the final discussions and from the participants. The meeting was very useful to see what areas the EC are focusing on with DLT Blockchain with SDN, IoT security and privacy, management and lifecycle (with need for standardisation in areas across the IoT verticals to give an integrated management and over the air updates). It was initially stressed how for instance, as far as standards are concerned often there is confusion on who is applying them, and which one are been applied, therefore a better coordination action might be needed. This would facilitate the sharing of best practices which can be also, in a later phase, included in a catalogue.

It would be good to give an appreciation of these tracks and the potential benefits and downsides they bring to IoT and specifically how they can benefit the LSP use cases considering the state of play of their deployments. For this it would be needed to have good insight into the security and privacy architecture and PIA outcomes and conclusions concerning the areas that they are addressing well and what mitigations they are having to address and areas that they just are not able to address just now and have to limit their use cases. It was suggested to have a workshop with the LSPs on this, but as a first step to have access to this data from the LSPs (possibly on a general level so it's more of a summary done by the LSPs across the board of each LSP).

The need for taking into account the context of the IoT use case, in terms of its risk assessment at each level (the device, gateway, network, edge, cloud, application, organisation) and appropriate treatment or not at each level (and taking into account the type of device (upgradeable, not upgradeable, wireless, wired etc)). Important the need to deploy IoT solutions that are upgradeable and able to factor in future security and privacy threats and address these through upgrades or extensibility. In summary several issues to be considered where raised: identification of gaps in the life-cycle management standards, identification of blockchain use-cases, explore sharing risk assessment.

Looking at the big picture it's important to realise that today there are many IoT devices as consumer goods such as Apple watches etc. and that these are mostly regulated by the GDPR, but are not subject to specific security or privacy standards, nor strictly controlled or monitored. And, as it was stressed during the meeting the GDPR is not the only legislation to have a look at, as there are other legislations applicable.

However, going back to the big picture IoT is only going to become more invasive in everyday life and permeate in all areas through the usefulness and efficiency it provide, so it must be considered that the security and privacy (and therefore trust in) of IoT devices are essential to the immediate physical security of persons themselves e.g. your IoT health monitoring devices are hacked and being monitored by malicious entities or are stopped from delivering essential data indicating a pending heart attack or that your autonomous vehicle is hacked and the driving habits are monitored or worse that they take over the driving of the vehicle and cause damage to persons. Thus, taking this view it is essential that standards for security and privacy in the area of IoT are continuously developed and linked with regulatory bodies to ensure compliance.

The impact of AI monitoring all IoT data should also be addressed and to be wary of the likability of datasets they have to and the potentials they have for deriving new profile sets that could be to the detriment of persons e.g. in the use of insurance companies.

Where there is sensitive data or mission critical data being processed it could be good to advocate the use of specific ISO/ETSI standards specific to IoT and also generic ones related to the organisations. The "AS-if" principle is important in this aspect that even systems not currently processing personal data should consider how their architecture should take into account processing of personal data so to make sure that it provides for future possible function creep and offer a higher level of protection for the data being processed.

As mentioned, it has been noted that there are many standards being developed for security and privacy in IoT and seen as very much dependent on industry whether they take it up or not. There is willingness from ISO and ETSI to consider LSPs feedback and this should be encouraged so to help make the standards relevant to the issues the LSPs are experiencing and highlight the challenges in providing security and privacy solutions specific to the IoT verticals, common to all verticals and across verticals. AIOTI can be also used for this purpose.

Additionally its needed to highlight how the standards are relevant and provide value so specific to EU ETSI can potentially be more optimal to address this with providing a set of security and privacy standards that help IoT ecosystems, organisations and, products comply with the GDPR and also consider how it can fit in with ENISA plans on security labelling and certification of ICT products, organisations, ecosystems. This is an area that it would be good to get also LSP feedback on this.

4.2 Summary

The workshop produced good results by bringing together different representative of the LSPs to address security and privacy to support common activities. The meeting generated a good interaction among the participants which had the opportunity to exchange solutions and approaches. The goal to bring the communities together and develop further the relationships based on the common needs and interests was achieved and further points of actions and improvement were identified.