Report on Workshop on Security & Privacy in IoT

13 January 2017

A. SUMMARY

On 13 January, the European Commission organised and hosted a follow-up workshop in Brussels. In this workshop, participants were asked to come with, reflect and comment on concrete minimum baseline security and privacy principles to create a trusted IoT environment.

The main purpose of the workshop is to discuss minimum baseline security and privacy requirements along the entire networked architecture and value chain similar in various sectors. The outcome of the workshop should contribute to cross-sectoral top 5 to 10 main baseline principles per IoT domain addressed during this workshop, being.

A. Wearables & Smart Appliances
B. Connected/Autonomous Vehicles
C. Industrial IoT
D. Smart Cities

The results of this workshop in these four domains show an aggregated thirty (30) minimum baseline principles regarding either security or privacy in IoT, or both, and of which numerous overlap cross-sectorial. These thirty principles also show that even though the four domains chosen are quite different from each other, the concerns and related main principles are actually applicable in each of the four domains.

Furthermore, the discussions during the Workshop showed a clear need to identify, structure, understand and address life cycles, including:

1. **IoT device/product life cycle** – what does the life cycle entails, how long needs and can a device/product remain connected to an IoT ecosystem in a secure, safe and compliant manner, what can the user/customer expect, and how is both the device/product as well as the user/customer able to keep up to date with (at least) the state of practice?

2. **Stakeholders life cycle** – what stakeholders are involved regarding an IoT device/product and in a relevant IoT ecosystem, what if the dynamics thereof changes, who is accountable for what part of the ecosystem, how to keep the stakeholders up to date, and what happens if there is an incident of any kind within the IoT ecosystem?

3. **Data life cycle** – what data is collected, created or otherwise concerned, what is its classification, can it be segmented, minimised and isolated, what if it has multiple classifications and what if the classification changes, how controls the data, for what purposes is one entitled to process the data, what meta data and derived data is generated during the data life cycle, and what does data deletion mean?

4. **Contextual life cycle** – in what context is a device/product used, as what persona is a stakeholder involved and in what context is data used in an IoT ecosystem, what if the context thereof changes, who is accountable in what context, how to make stakeholders aware of changes in best practices, rights and obligations when the context changes, and how to secure the rights and obligations of the relevant other stakeholders?

Taking into account the minimum baseline security and privacy requirements identified and discussed in the previous open sessions, being the 16 June 2016 Workshop and Digital Assembly in 2016, this workshop on the one hand acknowledges those from the perspective of the respective B2C and B2B ecosystems and deployment models in the four main domains zoomed into during this 13 January 2017 Workshop.

B. WORKSHOP BACKGROUND INFORMATION & OBJECTIVES

The Internet of Things ('IoT') – all-embracing heterogeneous networks of smart devices hyper-connected with each other via the Internet – is on the rise and will become reality within the next five years. The decisive change accompanying the IoT will be its ubiquity: networked devices are everywhere. Like any technological progress, this development offers social and economic opportunities, but at the same time it also harbours risks and detrimental impact. Notably, the IoT is transforming and disrupting our daily lives faster than any other technology before.

However, it is also a development that exposes users to increased risks and detrimental impact. In IoT every networked device is a potential target for hackers, marketeers and the like, and it is likewise a challenge to trace the data flows and functions actually carried out by so many connected devices and related ecosystems.

> In the IoT, every networked device is currently a potential target for hackers. Every day, there are reports of IoT-devices being hacked, ranging from control being taken over a vehicle up to interference with the functioning of an anaesthesia device. In the majority of cases, it is at weak points in the software that hackers manage to gain unauthorized access.
>
> No user of a networked device – either business or consumer – can be absolutely sure that the device only features those functions and only executes those data flows that have been specified by the persons or bodies authorized. Thus, for devices in the IoT, it is not possible to trace the data flows and functions actually carried out. A smart thermostat is a random yet good example where it is difficult to establish an owner of the generated data is and who controls where data is sent.

One of the policy challenges for IoT is to strengthen trust, security as well as personal data protection in the field of IoT.

One possible solution to this challenge could be the development of a 'Trusted IoT' label (as identified by the European Commission in its 'Communication on ICT Standardisation Priorities'), which will provide to consumers of IoT products information about the products' level of security and privacy. Such a 'Trusted IoT' label could be similar to the labelling system used today to indicate energy-efficiency of various appliances across the EU.

These need to relate to all sectors and cover the entire networked architecture or value chain from components of simple IoT-devices (e.g. smart thermostats) up to complex IoT-systems like connected cars and smart cities. These rules shall guide common tools and approaches such as standards, certification regulation and labelling.

It is intuitive to assume that with time most consumers' goods will be 'smart' and connected, embedded with sensors, software and network connectivity. If we analyse closely all the components of an IoT-based product, we can easily conclude that the end-user buys a fairly complex product, which involves interaction with third parties for its functioning, and at least the following elements, which layers shall be further elaborated as work continues:

1. A tangible element (e.g. the hardware)
2. Embedded software
3. Software maintenance
4. Supply of digital infrastructures or services (with long-term contract)
5. Procession and exploitation of user data

As ever shorter time-to-market in the hyper-connected world is crucial for the competitiveness of the European industry – which already lags behind its US counterpart – guiding rules defining conditions for security and privacy by design requirements are badly needed.

To strengthen trust of individuals, citizens, consumers, businesses, government and other persons and organisations on the demand side in their networked day-to-day and commercial life, which obviously also includes industry and other manufacturers and vendors that procure, deploy and use as customers as well, minimum baseline principles for security and privacy in the IoT domain are called for that minimize risk and detrimental impact while remaining open to innovation, and which are technology neutral and business model neutral.

Based on the EC Digital Single Market technologies and public services modernisation package published on 19 April 2016, the European Commission is asking about IoT relevant Actions from Standardisation Communication. A workshop was organised by AIOTI on 16 June 2016 in Sophia Antipolis, France, during the ETSI Security Week 2016 to explore the options and guiding principles to come to minimum baseline security and privacy requirements. Subsequently, at the Digital Assembly 'Internet of Things and ePrivacy' workshop on 28 September 2016 these topics were discussed as well, where AIOTI WG4 'Digitisation of Industry policy' issued a related document that was taken into consideration as well.

On 13 January, the European Commission organised and hosted a follow-up workshop in Brussels. In this workshop, participants were asked to come with, reflect and comment on concrete minimum IoT privacy and security principles to create a trusted IoT environment.

The main purpose of the workshop is to discuss minimum security and privacy requirements along the entire networked architecture and value chain similar in various sectors. The outcome of the workshop should contribute to cross-sectoral top 5 to 10 main baseline principles per IoT domain.

C. PRESENTATIONS & BREAKOUT SESSIONS

The Workshop started with keynotes and other presentation, where after four breakout sessions where convened in the following domains:

E. Wearables & Smart Appliances
F. Connected/Autonomous Vehicles
G. Industrial IoT
H. Smart Cities

As Deputy Head of Unit IoT, Nikolaos Isaris, who opened the Workshop, stated the Workshop is meant to identify, discuss and come to concrete minimum security and privacy baseline requirements to strengthen trust, also as currently various IoT devices and ecosystems are wildly insecure. Head of Cybersecurity & Digital Privacy Unit, Jakub Boratyński, who co-opened the Workshop amongst other topics addressed the need for trust, confidence and cyber resilience in IoT. Head of Sector of Unit IoT, Rolf Reimerschneider stated in his key note that each stakeholder in the IoT value ecosystem needs to consider incentives for customers/users to buy and use secure IoT products and services, where he also mentioned that the market apparently needs more hacks to further raise awareness.

The presentations of the speakers that gave permission for publication thereof are made available on the relevant webpage of the European Commission. The four breakout sessions at the workshop each focused on an IoT domain for which these principles are relevant, in which each session the top 5 to 10 baseline principles were identified, discussed and prioritised. This report summarizes the results of the four breakout sessions.

1. BREAKOUT SESSION WEARABLES & SMART APPLIANCES

This breakout session covered the minimum baseline security and privacy principles in the domain of wearables & smart appliances.

As there was not much discussion on the scope of this domain, the participants were able to dive into the issues, scenarios, barriers, impact assessments and potential measures and prioritized requirements to help strengthen trust.

For once, quite some recent examples of hacks and other security and privacy breaches or other cases where mentioned such as (i) a vulnerable series of pacemakers and the intervention by the FDA, (ii) security flaws in generally available routers and cameras and the intervention by the FTC, (iii) the murder case where an Amazon Echo is a stakeholder regarding possible evidence, (iv) Uber considering to share personal data of its customers/users with authorities, without legal necessity, (v) the IoT-enabled DDOS attacks on DYN, and of course (vi) the two connected toys with no security measures in place and and severe personal data protection and consumer protection implications.

It was for instance established that because of IoT and the arising challenges and problems, one is not trying to solve problems that were already present but were not addressed and not solved before, where because of the hyper-connectively of IoT as well as its connection with cloud computing and data analytics those challenges and problems are increasing rapidly.

In order to now address and solve these, while nurturing innovation and social inclusion, the normative angle was discussed to both identify minimum based line requirements and set the height thereof, which norms includes a relatively high level of baseline (i) when safety is at stake, (ii) when critical infrastructure or national safely can be

materially impacted, and of course (iii) when mandatory law is already of will be applicable.

After a breakthrough exercise with all participants involved, the following top 7 minimum baseline security and privacy requirements that surfaced in this breakout session on wearables & smart appliances were identified:

1. **Data control by the user** – in any phase of the data life cycle and product life cycle

2. **Transparency and user interface control** – empower the user to obtain sufficient knowledge on what its devices and related system are doing and sharing, even if it concerns M2M communications and transactions

3. **Encryption by default** – in communication, storage and otherwise

4. **Relatively high level of baseline** – when safety is at stake, or critical infrastructure or national safely can be materially impacted

5. **Life Time Protection** – give security, safety and privacy protection over the full life time

6. **Updatability** – trusted and transparent updates only by authorised parties, not by malicious actors

7. **Identity protection by design** – decoupling personal identity from device identity

2. BREAKOUT SESSION CONNECTED/AUTONOMOUS VEHICLES

This breakout session covered the minimum baseline security and privacy principles in the domain of connected respectively autonomous vehicles.

As there was not much discussion on the scope of this domain – the vehicle was seen and addressed as a sensing, actuating, communication and data processing platform on wheels –, the participants were able to dive into the issues, scenarios, barriers, impact assessments and potential measures and prioritized requirements to help strengthen trust, where it was noted that security and privacy were not seen as a barrier to innovation, and no privacy would be possible without security.

The topics data control, access and use were discussed, including who should have control over what data, this as per the various stakeholders, such as drivers, passengers, vehicle owner, peer-to-peer sharing persons, manufacturers, service providers and so forth.

On personal data and privacy, the following top 5 minimum baseline principles in IoT that surfaced in this breakout session were identified, in no particular order:

1. **Data segmentation, also within the domain of personal data** – as per the context of the personal data, the multiple personae each data subject has, and the related protection – including fundamental and consumer rights – it has

2. **Data control, assess and use to be defined** – as per the various stakeholders, such as drivers, passengers, vehicle owner, peer-to-peer sharing persons, manufacturers, service providers and so forth

3. **Transparency as primary requirement** – awareness, informed and unambiguous consent per contextual processing of personal data (which data for which use)

4. **User control** – choice of the user: possibility to opt-out, data subject right to access their data and portability right of their data, communication platform to control data access and to ensure security and privacy, and the overall securing of personal data processed, not only in and by the vehicle, but also in the context of related systems and devices (e.g. navigation-satelite)

5. **Privacy by design and privacy by default** – earmarking data collection, ensure data minimisation, and the ability to hold liable the manufacturer or service provided for misuse of collected personal data

On security, the following top 5 minimum baseline principles in IoT that surfaced in this breakout session were identified, in no particular order:

1. **Harmonised industry approach** – standardisation of the functional and security assurance requirements through common harmonised industry approach: 1) in which every control unit is to be protected and 2) connectivity unit such as vehicle information control and access control) to benefit from a higher protection

2. **Harmonisation approach** – reduce the impact of different national regulations

3. **Updatability and upgradability ("security as a moving target")** – use of related securitisation processes with 1) need for regular updates and upgrades during the vehicle lifetime, and 2) need to use identifiers for an adequate identification of devices

4. **End of support** – where the current practice is about 12 to 15 years, the end of life cycle and the related support is prerequisite. Questions to be addressed are: what happens if a services agreement is lawfully terminated, is there an update possibility, when will updating and upgrading become limited, and who is accountable for the risk of not updating IoT devices and systems

5. **Identifying and securing interface points** – also to reduce the risk of security breach

3. BREAKOUT SESSION INDUSTIAL IOT

This breakout session covered the minimum baseline security and privacy principles in the domain of industrial IoT.

The industrial IoT domain summarizes everything what is outside the classical consumer domain. In general terms it focuses on the entire networked architecture of industrial control systems and decision support for processes and operations and related value chains on a cross-sectoral level. The reliance on Internet-connected control systems, specifically on the interconnectivity between operational, industrial and information technologies has changed and expanded the potential of vulnerabilities. While industrial IoT in its core targets delivering critical services and support for B2B operations, a potential IoT security risk affects an organisation’s business, assets, also health and safety of individuals and the environment.

Actually, industry has put in place established safety standards and related procedures

to implement. Quite broad, long-standing experience on safety regulation and standards are available for almost all relevant industrial sectors. Safety standards have to be in place before an industrial system starts operations and little changes are happening during production lifecycle. In contrast, security has a much more dynamic character and related standards are much more difficult to dynamically adapt.

To manage industrial IoTshop floor risks, a clear understanding of the organisation's process chain and security considerations specific to be use of the connected IT and OT is required. Risk management is an ongoing process of identifying, assessing and responding to a risk. In an industrial context, priorities of industrial IT security require to guarantee system operation and ensure system integrity in terms of:

1. functional safety and integrity
2. System availability with no loss on productivity (KPI in manufacturing)
3. Accountability - legally required evidence and fault identification
4. Confidentiality (protection against IP espionage, product piracy and know-how theft)

To manage these kind of risks, organisations would have to understand its nature, identify the likelihood and weakness of all elements of the chain and the resulting impact. In this context, the definition of a *reference architecture model* could help to define security requirements across various sectors. The architecture model would have to cover tangible HW components, machines, embedded SW, industrial control systems, communication interfaces, the network infrastructure as well as the data storage and analytics plane. It would help to analyse possible evolving risks and possible risk mitigation measures from component to application and data level.

Because the system architecture may vary across verticals, the tools and methods used to achieve the security and risk management described by *a security framework* may vary across different verticals. The analogy of architecture model may help to do find kind of mapping and identify possible synergies in risk management.

Before deploying industrial systems, specific considerations on cyber security would have to take into account at the time when the architecture is designed and its component interfaces are developed. *Security by design* has given the highest recognition, as it is not effective to patch security measures after system deployment, e.g. there is great need for comparative security investigation into basic software structures & frameworks and their design principals to tackle weaknesses and exploits from the past. With evolving degrees of digitisation the trend to even more complex networked systems is even amplified. A security architecture model may simplify the system assessment and allow a better understanding of the relationship between security risks and mission-critical objectives such as safety and functional requirements. By all means, a security assessment would have to cover all components of the architecture of a connected system, while taking the life cycle of the device into account.

Recognising the important role of security and safety for B2B processes, security standards played a pivotal role in the discussion. It is clear that breaches in security inevitably cause safety risk for industrial systems – it was nevertheless also clearly stated that the verification, certification of functional safety rely on established standards that are shared across a large variety of industrial systems like energy, automation, logistics, transport. Safety design, verification and its compliance to relevant standards need to be shared across the supply chain – and this process will happen likely before a systems starts operation.

International security standards have to be supported across all actors of the supply chain to be effective. Security principles, on the other hand, would have to be defined for all levels of the device including components, firmware, application and communication

between the devices and towards the cloud, and shared across an ecosystem. This make a risk management across supply chains feasible though requires for each actor an enterprise-wide approach to manage risk via agreed actor-level risk management policies, processes and procedures. This likely includes a Third party governance structure (e.g. risk council such as BSI in Germany) with the skills to perform the appointed security risk management responsibilities. The independent third party organisation makes sure that risk procedures, processes and risk management are implemented consistently, so it manages security risk at supply chain level, defines procedures and performs audits. Such a council requires formal agreements in place to communicate baseline requirements to its suppliers and monitor their implementation.

If IoT is implemented in the remits of a functioning ecosystem (with agreed security processes and procedures)– it is feasible to find a broad agreement on interoperability standards – to exchange information of security breaches /keep transparency on risks Reference has been made to define KPIs through a *trustworthiness framework* that is agreed across all relevant suppliers. Each organisation in the process chain knows its role in the larger ecosystem and has agreed on the standard-based procedures to interact and share information. Such a framework must be technology neutral to be extensible and able to adapt to latest technology innovations and also different levels of attacks. Agreeing on trustworthiness levels required for contractual arrangement within the ecosystem or vertical. In contrast, an agreement on a security framework for connected services that build on open APIs and cut across verticals is not straight forward and actually not in line with current vertically oriented development processes.[1]

The principle that is unique to security, however, is its dynamic nature. For security, a continuous risk monitoring and approach validation is necessary over a production lifecycle. Basic security principles have to be continuously monitored and maintained over potential long cycle of industrial operations – which is a huge challenge by itself. Any security framework has to follow latest trends in cyber-attack and has to flexible respond to dynamic changes of cyber-attacks and a varying nature of possible hacks. Consequently, security design and verification requires continuous monitoring at global level with a need to flexible up-date and adapt the security framework in place during the entire production lifecycle. This principle is much different of current state of play of product support and requires continuous effort for monitoring and maintenance of any component, product or service delivered and eventually the definition of product lifetime (end of warranty means end of support but not necessarily end of use). This Supplier Code of Conduct, manufacturing suppliers and system vendors would have to bear in mind when designing connected or Industry 4.0 products.

Based on the above, the participants dived into issues, scenarios, impact assessments, potential measures, and other requirements to help strengthen trust. Trustworthiness was established one the main quality KPIs in this domain.

Regarding privacy, both the legal frameworks and respective requirements arising out of the GDPR as well as the ePrivacy directive/regulation where identified as baseline privacy and security requirements.

The top 6 minimum baseline security principles that surfaced in this breakout session were:

1. **Sustainability** – connected devices as well as any IoT component as defined above need to be durable and maintained as per its purpose, context and respective life cycle;

[1] Example: a combination of smart meter and smart home apps rely on different trustworthy principles. Second example: the current practice of consumer IT systems in hospitals. Medical equipment undergoes a certification, the IT infrastructure not which cause dramatic risk for patient data and hospital operations.

2. **Transparency and accountability** – empower the stakeholders to know what the devices and ecosystems are doing and sharing, and why; agreed KPIs and trustworthiness levels would complement the contractual arrangements for product or service provision. Suppliers Code of Conduct has been agreed across an ecosystem – where an independent authority might greatly help to ensure consistent implementation of security principles.

3. **Security by design -** given the complexity of connected industrial systems would benefit from the definition of *a reference architecture model*. – to agree on security standards, procedures, processes and risk and impact management

4. **Security by default.** proven, well understood and securely up-datable settings are indispensable before starting operations and during IIoT life time (Security is not static, cf. Assurance)

5. **Assurance** – component and system suppliers need to be prepared for security monitoring and system maintenance over the entire life cycle and need to provide end of life guarantees for vulnerabilities notifications, updates, patches and support

6. **Separate Safety and Security –** Safety principles have to implemented and validated, separately from security principles

4. BREAKOUT SESSION SMART CITIES

This breakout session covered the minimum baseline security and privacy principles in the domain of smart cities.

As there was quite some discussion on the scope of this vast domain that is summarized as smart cities, the participants first zoomed in on the scope they wanted and could discuss in order to then deep dive into the issues, scenarios, impact assessments and potential measures and other requirements to help strengthen trust.

The top 8 minimum baseline security and privacy requirements that surfaced in this breakout session on wearables & smart appliances were:

1. **Human-centric –** security and privacy should be universally applied to data subjects

2. **Data isolation** – functional separation of datasets and databases

3. **Transparent roles** – ensuring clear allocation and identification of roles, including who is data controller, co-controller, processor, co-processor, and so forth

4. **Single point of contact** – provide single point of contact for personal data protection and privacy

5. **Non-discriminatory practices** – ensure non-discriminatory practices against data subjects (citizen and any other persona such individual may have while being part of the ecosystems of a city) and businesses on the basis of information derived from IoT deployments within smart cities

6. **Independent privacy and security audits** – cities of a certain size should

mandatorily carry out thirds party privacy and security audits

7. **Dynamic trust KPIs and metrics** – on security, privacy, safety, resilience, reliability and the like

8. **Continuous monitoring** – ensure continuous monitoring and improvement of IoT ecosystems, including clear metrics and measurements