DEVICE-CENTRIC IOT SECURITY RISK SPECTRA MAPPING TOOL

EIGHT (8) QUESTIONS & ANSWERS ABOUT RISK, RISK CLASSIFICATION AND THIS TOOL

1. What is Risk-Based?

Having a risk-based approach is second-nature for human beings, and nowadays - in this Digital Age - a need to have. It is being used and implemented more and more in the various markets where connectively, inter-connectively or even hyper-connectively play a role. It is also the current and well-known approach for every Digital Decade 2030 policy initiative and instrument.

Each situation and context create different risks. These have different risk levels, that ethically, societally or otherwise justify different risk mitigation measures and appropriate levels of accountability.

2. Where to Start?

So, we need to start with identifying what risk means, and classify the risk per context.

3. What is Risk?

Risk is not a four-letter word. Risk is the dynamic equation of (a) the probability of occurrence or event, times (b) the potential adverse impact, within a particular context and its periphery (both the cyber, cyber-physical and physical domains). It is dynamic, changes over time, so also requires dynamic risk classification mapping.

Risk classification, based on context, therefore is an essential starting point to identifying and thereafter mitigating cyber threats. The developed Risk Classification Spectra Mapping Tool provides such guidance, in an agnostic and neutral way.

4. Why IoT device-centric?

It has an IoT device-centric approach, for the risk and risk classification mapping to have good yet understandable focus. This, as the challenge is that devices are often used for or otherwise part of various use cases and situations which are associated to different risks being mapped to different risk levels. It therefor makes sense to starting at connector-level of an IoT device, and then taking in and layering up other risk spectra, such as functionality, data flows, application, intended use, sector, and so forth.

5. What to Verify & Assure?

The Device-Centric IoT Security Risk Spectra Mapping Tool supports you with plotting and mapping what risk to verify and assure.

It has been developed and established in collaboration with Arthur's Legal, TÜVIT & IoT security community. It provides guidance on the layered, multi-layered and holistic Risk Classification of IoT Devices and the (eco)systems those devices are connected to or otherwise part of. Next to security risks, other risks are taken in as well, including safety, privacy, financial, economical and ecological risks.

The Tool is provided as-is and free of charge, based on Creative Commons BY-NC-SA, and consists of three files:

A. This Q&A Introduction;
B. How to Use Guide (Seven Step Protocol), which includes the Device-Centric IoT Security Risk Spectra, and
C. Mapping Table Device Centric IoT Security Risk Mapping Table, which is made available in Excel.

6. For Whom?

Where any market or ecosystem consists of both demand and supply side but also users, society, policy makers and other stakeholders, this Device-Centric IoT Security Risk Spectra Mapping Tool aims to support any and all stakeholders and perspective it may have. For instance:

A. Manufacturers, integrators and partners are supposed to implement technical and organisational cybersecurity measures based on a risk assessment;

B. Customers, users and society are supposed to be able to ascertain that appropriate risk-based cybersecurity measures have been implemented, and understand how to trust, and based on what;

C. Procurement departments need guidance to understand risk classifications by manufacturers and others in order to be able to procure devices and ancillary services which cover the risks they are facing in their individual use case, and;

D. Policy makers and authorities are supposed to be able to understand, give guidance and monitor which appropriate, contextual risk-based cybersecurity (existing, upcoming or envisioned) policy initiatives and instruments make sense, are feasible and (to be) implemented.

It brings quite some positive value and increased trust for the manufacturer, the procurement departments, customers and policy makers to have a common understanding of risk classifications.

7. What other brief backgrounds can be provided?

For instance, the development process is requested to start with a risk assessment in order to be able to decide on required cybersecurity features which mitigate risks associated with the intended use case. A harmonized standard on the risk classification could support the developer as well as the procurement departments – and many others – to benefit from similar interpretations of risks associated to the device and ancillary services. An assessment of implemented cybersecurity features gives trust to the proper implementation and information would be able to be visualised to what kind of risks the device and ancillary service has been prepared for.

Additionally, a harmonized risk classification would reduce a deviation within the European Single Market (and beyond) in order to circumvent interpretations of risks while taking various Risk Spectra and Risk Layers into account. Risk Spectra and Risk Layers reflect various stakeholder' views including manufacturer, operator or public interest while looking at individual components implemented, connectivity used, data generated or transferred, in which environment operated, financial impact, usage, and many others.

A joint understanding of risk classification of IoT devices and ancillary services is necessary in order to benefit from the various legislative requirements in place and in preparation. A Risk Classification would fully fit into the European cybersecurity framework with the Cyber Security Act (CSA) and its Cybersecurity Certification Framework, the NLF with the Radio Equipment Directive (RED), its Delegated Act regarding connected products, Machinery Directive, GPSD, Medical Device Regulation and envisioned Cyber Resilience Act (CRA).

8. What is the Call for Action?

There is no particular call for action, except for: (a) please use it at your discretion, (b) experiment with use cases, (c) share your use case risk classification outcomes, good practices or other learnings where and when you wish to, or (d) send us your other feedback you may have. Thank you advance!

Reminder. As a reminder please do note that this is the Device-Centric IoT Security Risk Spectra Protocol, focussing from a single device. Hence, when more devices, systems and services are relevant – which is generally the case in deployed IoT ecosystems – it is recommended to also run this Seven Step Protocol, in a layered way, with multiple devices and related technical stack, stakeholders and the like. Layered, as with that one can both better identify and address the dependences, risk aggregators and risk mitigators, as well as later on better identify and pinpoint threats and vulnerabilities and its potential impact thereof. It also demonstrates that manufacturers and operators of (parts of) IoT ecosystems – and customers and other demand side of (parts of) IoT ecosystems – might have different results in their risk classification of selected IoT devices.