The PP will bring Harmonization to the way security functionality is described

When it comes to IoT cybersecurity labels are a hot topic in lots of regions around the world (Singapore, UK, EU, etc). One interesting part will be how the label is baselined. A smart choice would be to use the existing NIST 8259 minimum security requirements which have a lot of industry attention already. The label might in addition introduce a level concept (e.g. 1 to 3) in a similar way to white goods energy ratings. One other interesting point is how vendors will prove that they have followed these requirements. For the lower levels this might be done by self-declaration, whereas the higher levels might require independent validation by a test house like UL or SGS. The latter would require the definition of a test concept and standardization of test vectors to enable subjective testing. This is where it might become complicated. Since the higher labelling levels would likely target a greater assessment depth with deeper testing, the IoT devices in scope on the other hand will each be feature rich and complex. Thus making the efforts per IoT device high and in turn the approach hardly scalable.

Looking at IoT devices they all rely on a central control unit. This control unit comprises of several hardware components, associated firmware and software running on the components. This IoT control unit usually contains a large MCU or System on Chip and a Real Time Operating System, memory storage units, it also contains communication hardware and the software stacks associated with the communication protocols. The role of this control unit is to handle the main functions of the end IoT device like to onboard the device to the cloud by setting up a secure channel to a trusted end point, verifying its own unique identity, downloading configuration data and software updates. Such central control units are the brain of each and every part of the IoT from a robot vacuum cleaner to a robot in an industrial manufacturing plant, it is in charge of security and safety of the IoT device.

Global Platform have developed an evaluation methodology called Security Evaluation Standard for IoT Platforms or SESIP for short. This standard and associated methodology was developed with the IoT Controller in mind. SESIP is cost effective, takes into account time to market and is flexible enough to cover all aspects on an IoT Controller including MCU, Software, Secure Memory, communication chips and sensors. SESIP is flexible enough to cover innovation allowing standardization groups to define industry testing norms around security topics. We see this as an important step to bring security testing and therefore trust into the unregulated IoT domain. So let’s look a little deeper at SESIP and why it is an important step in bringing trust to the IoT.

We start by looking at the 2 key layers or sub-components of an IoT control stack a hardware layer (Security MCU) and a Software control layer (FreeRTOS) and will then be looking at the vendor of the IoT device.

A Security MCU provides essential root-of-trust protection for an IoT Controller. This can be used to perform cryptographic operations, uniquely identify the component (secure ID), store sensitive user data, provide support to authenticate the device and verify that the cloud service requesting access logically to the device is genuine. Some important security features commonly placed in a Secure MCU include. The security MCU is often defined as a Root-of-Trust this simply means that it is used as the key component to authenticate operations sign and verify external parties and store essential security data including user data and cryptographic essentials keys and signatures. Global Platform has released a SESIP Profile aimed to harmonize the security requirements and services that a security MCU can provide. A SESIP Profile is a set of agreed industry norms, and allows a common requirements list that a security MCU must have and a common way of describing the functionality present with a compliant device, it also allows harmonized testing to be performed across various test houses. The main security features of MCUs/MPUs covered by the SESIP Profile are:

- Secure initialization, to control the platform’s initialization sequence.
- Secure update.
- A strong identity anchored in the MCU/MPU.
- Secure debugging in case of investigation need; optionally auditing and logging features can also be implemented.
- Cryptographic services, often based on hardware cryptographic accelerators.
- Hardware protections to handle hostile environment, if needed by the use case.
- Isolation mechanisms controlling access between different parts of the software building the product.

This harmonization allows an IoT device vendor to easily sort and understand what the secure MCU offers and how it has been tested.

Software control layer – IoT solution developers building applications on FreeRTOS desire software contiguity and continuity because it reduces integration and system update risk. When the solution developer brings together software contiguity, software continuity, and FOTA, an effective IoT device relationship emerges. IoT solution developers want software contiguity when identifying related software components. Software contiguity asserts a well-known, contiguous set of software components, ensuring that the related software component versions have been rigorously tested together. IoT solution developers want software continuity when maintaining applications. Software continuity reduces application code churn since it ensures no application programming interface (API) and breaking changes from one maintenance release to the next. No API or breaking changes reduces implementation and integration risk since an LTS maintenance release should not require application changes when integrating the maintenance release.

Let’s discuss what this means for an OEM developing an IoT device. The SESIP community has developed an IoT device SESIP Profile that matches the NISTR 8259 and ETSI 606 345 baseline requirements for IoT devices. The SESIP Profile is targeted to be very user friendly. It targets the IoT device vendor as user and makes it as easy by means of being a questionnaire to fill out and create the SESIP Security Target of the vendor’s IoT device. With mappings from other SESIP profiles like the Secure MCU Profile to this IoT device Profile it allows the IoT device vendor who is using a certified chip to support or negate test cases in the IoT device profile since these are already covered by an existing certificate. The same holds for other profiles like for a software SESIP Profile generalizing security requirements and services of a real time operating systems.

With this approach apply the cybersecurity label to the IoT device vendor and also include their suppliers and sub-components it enables more comprehensive labels based on more rigorous assessments and testing. At the same time this incentivizes to build more secure devices by using already secured components since it will ease the overall compliance demonstration for the IoT device vendor. This approach will also enable more harmonized testing across the layers of an IoT control stack.