Answer to : Call for Papers on Consumer Software Labeling from NIST

.

About TÜV SÜD: we are a third party laboratory with experience on labelling for consumer IoT products with projects on going or completed with Finland Trafficom label, Singapore CLS label, TÜV SÜD own label CSC. Moreover, we have a long history to provide testing, certification and labelling for a wide area of products on different scheme worldwide.

Suggestions and feedback on the challenges and practical approaches to consumer software labeling

1. *Formal and informal processes and practices used to secure the software development process*
    a. The challenge to provide proof of compliance to a secure software development is that it is not necessarily testable on the IoT itself and it is needed to provide to a lot of other documentation.
    b. Our suggestion is not to evaluate the secure dev process but to find test points in a product that will show indirectly that there is secure dev. Example of test points : the software is securely updatable, contact point to report vulnerabilities, different API key and secure storage.
2. *Technical criteria needed to support validation of consumer software security assertions that reflect a baseline level of secure practices*.
    a. Regarding the validation method:
        i. There should be a test report with a result that would indicate clearly which label tiered is applicable.
        ii. The test report should have a template
        iii. There should be a detailed test method with the test method to ensure test reproducibility.
    b. There is a choice to make between technical criteria that apply to all consumer IoT or select sets of criteria for various type (TV, Camera, etc.) of product.
    c. Technical criteria can use the NIST IR 8259A but the method should be more detailed to ensure test reproductivity.
    d. IoT devices are part of an ecosystem, so it might interesting on the label to explain that the webapp and cloud have been evaluated or not.
3. *How different conformity assessment approaches (e.g., vendor attestation, third-party conformity assessment) can be employed in consumer software labeling efforts*.

   a. If vendor is authorized to self-declare conformity of their product it is necessary to enforce a strict control by auditing thousand of products every year to ensure the self-declaration is taken seriously by vendor.
   b. It is also necessary to consider the accreditation of a vendor/third party lab and what should be the requirement to get the accreditation for example a lab should have the ISO 17025 and 17065 but for cybersecurity it doesn't really apply: how to "calibrate" Burp Suite?

4. *Consumer product labeling programs for educating the public on the security properties of consumer software*
   a. It is necessary to run an advertising campaign (website+ TV information+ newspaper) to inform the public and legitimate the label as the "official label"
   b. There could be different size of the label with difference level of detail depending on where the label is (on the product itself or on the packaging).
   c. Also, for the official launch of the label it would better that 50-100 brand run the test pilot so there is at least 50-100 compliant at launch, because a lot of label fail to be credible to the public and vendors when at launch there is only a few product compliant.
5. *Feasibility and possible means for implementing tiered labels that reflect increasingly comprehensive levels of testing and assessment*
   a. Due to the variability of consumer product, their complexity, their differences in intrinsic financial and cyber value it seems necessary for the label to be tiered.
6. *Measures for incentivizing participation by consumer software developers.*
   a. Incentive can range from nothing to interdiction to enter USA market.
   b. Transition period should be sufficient for the market to consider any mandatory labelling.

Other comments:

There is worth reading papers on the topic :
https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-pardis_emami_naeini.pdf