BlackBerry.

August 17, 2021

National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899

Re: Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software

Dear NIST,

BlackBerry supports NIST leadership in initiating labeling efforts to identify IoT cybersecurity criteria for a consumer labeling program and secure software development practices or criteria for a consumer software labeling program, pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity. We appreciate the opportunity to share our views and look forward to participating in the workshop on Cybersecurity Labeling for Internet of Things (IoT) Devices and Consumer Software on September 14-15.

Our position paper addresses several aspects related to cybersecurity labeling programs. Specific recommendations for the secure software development process include binary composition analysis and use of a software bill of materials (SBOM) to monitor for reported vulnerabilities in the software stack. We provide support for the concept of multiple "tiers" to enable consumer programs covering a wide range of the consumer devices to grow and meet the needs of small business and enterprises. We also note the importance of international harmonization for the global consumer IoT market.

Respectfully Submitted

James Lepp

James Lepp,
Senior Manager, Standards

BlackBerry Position Paper
Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software

1. Secure Software Development Practices

We recommend the use of a software bill of materials (SBOM) for pre-market and post-market cybersecurity analysis of embedded/IoT software. Industry references to SBOM already exists in guidance such as the CSDE C2 Consensus[1], although at that time was not included in the baseline recommendation. More recent advancements such as NTIA's SBOM Minimum Elements[2] have improved the state of the art in 2021.

An important first step in secure software development is identifying all the software that is being used in a product. Embedded IoT software is built from board support packages, binary drivers, SDKs, and other libraries. This includes a large dependence on open source software. It is important to identify all software components included in the end-product. Maintaining the inventory of all software components built into a product including their identity, versions and source should be a minimum requirement for the secure software development lifecycle process. A combination of source code management systems and binary software composition analysis can be used to automate the generation of this information.

We recommend binary composition analysis on the output of the build process as a way to validate that the correct source code was built, and that it was built with the correct configuration such as compiler defenses. In addition to generating or validating an SBOM, binary composition analysis can detect software of unknown provenance (SOUP) and detect secret leaks such as passwords and private keys in embedded firmware.

The SBOM can be provided and checked via self-assessment or third-party audit for completeness and accuracy as a certification requirement. This is applicable to both embedded software on consumer IoT devices as well as the secure development process for consumer software.

Many IoT Cybersecurity programs include a requirement for a software update mechanism to provide security fixes to devices already in the market in which significant vulnerabilities have been discovered. The manufacturer can use the SBOM to monitor for new CVEs and inform the patching process. An impact assessment guideline should define criteria for a significant vulnerability. Also, on the topic of software updates, a device labeling program will need a process to address whether the changes in a new software version require re-assessment of the product to maintain the validity of the label/certification.

2. Multiple Tiers and Assessment Methods

Having a program with multiple tiers is advantageous for several reasons. While the target of the program is consumer products, we expect IoT devices intended for consumers will also be attached to enterprise networks. Having a multi-tiered labeling program could allow the requirements to scale up to higher levels of cybersecurity risk mitigation for government and

[1] https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[2] https://www.ntia.doc.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials

regulated industry customers as well. The labels enable the customer, whether a consumer, small business, or large enterprise to choose the IoT product that fits their risk profiles.

In the European region, ETSI has developed a consumer IoT baseline standard and is also developing profiles for specific product categories[3]. For example, connected door locks and home gateways have a different level of security requirements then a smart lightbulb. We note that the NISTIR 8259 series and ISO/IEC 274xx series are also structured to enable multiple profiles. The availability of such profiles should be leveraged by the consumer labeling program.

The labeling tiers can be supported by a diversity of assessment mechanisms. For example, self-attestation for a lower tier and third-party conformity assessment for a higher tier. In this way, both the requirements themselves and the assessment are tiered. This gives vendors choice in how to position products they put on the market.

We note that the approach in other jurisdictions is to concentrate on the lowest tier first in an effort to dissuade completely insecure products from entering the market. Should this be the case with NIST's recommendations on consumer IoT device and software labeling program, we ask NIST to at least plan for a multi-tiered labeling approach so cybersecurity can increase over time and additional customer categories' (e.g., small business, enterprise) cybersecurity needs can be addressed.

3. International Harmonization

The market for IoT devices is global and device makers sell the same product in many countries and regions. Today several national or regional labeling programs are in existence or in development. We encourage NIST to take this into account and harmonize their guidance with publications like ETSI EN 303 645, the ISO/IEC 27402 and NIST's IR8259 series. These standards are in various states of publication and revision as the IoT market continues to evolve rapidly. We recognize NIST Online Informative Reference program (OLIR) and its progress that mapped several industry publications to NIST IR 8259A. Continuing the effort would increase industry participation in the labeling program.

In addition to requirements standards, industry developed open and publicly accessible test/assessment specifications allow manufacturers to check their compliance in a cost-effective manner. The ETSI EN has an accompanying ETSI TR 103 701 assessment specification for this purpose. NIST should delegate a standards body to develop test/assessment specifications for the labeling program.

4. Summary

We have addressed several aspects related to cybersecurity labeling programs. Specific recommendations for the secure software development process include binary composition analysis and using a software bill of materials (SBOM) to monitor for reported vulnerabilities in the software stack. We support the concept of using multiple "tiers" to enable the consumer labeling program to grow and meet the needs of small business and enterprise customers. We also note the importance of international harmonization for the global consumer IoT market as the IoT industry continues to grow and evolve.

[3] https://www.etsi.org/technologies/consumer-iot-security