August 17th, 2021

To: labeling-eo@nist.gov

The Open Connectivity Foundation (OCF) respectfully submits the attached whitepaper detailing the requirements of a comprehensive, practical, and effective approach to creating a program for consumer software and IoT labelling.

If you have any questions, please contact staff@openconnectivity.org.

Regards,

Mark Trayer
Chairman of the Board, Open Connectivity Foundation

Open Connectivity Foundation
3855 SW 153rd Drive, Beaverton, OR 97003 U.S.A.
TEL: (503) 619-0673 https://openconnectivity.org/

Leveraging Existing International Standards, Open Source and Certification Programs to Accelerate NIST's Timeline to Secure Products in Market.

By: Open Connectivity Foundation

Abstract

By working closely with existing international standards bodies, like the Open Connectivity Foundation, that concurrently provide cybersecurity software specifications, open-source implementations, and conformity assessment and certification, not only can NIST leverage existing industry-developed requirements to establish their consumer software label, but there is an opportunity to dramatically shorten the time until they see labeled products in market by leveraging existing open source and conformance programs to provide joint certification.

Introduction

Any approach to software security labeling, especially as it applies to the software that runs on Internet of Things (IoT) devices must be firmly anchored in the three tenets of secure software design found in a holistic standards-based development process: (1) an industry developed, peer-reviewed and internationally recognized specification that implement the appropriate security criteria, (2) an open-source program that delivers a reference implementation of the spec, and (3) a comprehensive conformity assessment program with rigorous testing and certification procedures.

Without rigorous conformity assessment, the security label provides a hollow promise and little, if any, meaningful information to buyers, fundamentally undercutting the value of both the label and its underlying security criteria. But when backed by rigorous conformity assessment, a security label has the potential to provide buyers with the information and confidence that the product meets or exceeds the security criteria underlying the label, enabling competition and market forces to help drive improved security in connected devices.

Background

The standards-based development process begins with an industry developed, and peer-reviewed specification from an international standards development organization (SDO). This specification forms the normative foundation upon which a comprehensive testing and certification program is built, with each requirement in the specification directly reflected as a test that is run in the certification and testing framework. The triad is completed by an open-source reference implementation of the specification manifested as code that conforms to both modern secure software design and passes the tests that certify conformance to the specification's requirements.

This process combines all of the essential ingredients necessary for a comprehensive approach to software labelling that includes standardization, implementation, and certification. All of this must be done in an open and collaborative manner that leads to publicly available specifications and code with a transparent software bill of materials.

Implementing a Security Label that Adheres to the Tenets of Secure Software Design via the Open Connectivity Foundation

The Open Connectivity Foundation (OCF) has used the process described above to create the OCF label built upon detailed specifications that incorporate modern cybersecurity criteria into IoT devices. Crucially, these specifications have also already been adopted as international ISO/IEC standards, paving the way for their usage across borders as a common baseline for IoT security that can be leveraged by national programs. Additionally, an open source and freely available reference implementation was developed in lockstep with the specification, essentially enabling device manufacturers to "compile their compliance" to multiple national security baselines *without* having in-house security expertise. This reference code must pass all 119 certification tests for the requirements it implements, including 60 security specific tests, confirming the security controls set forth in the specification have been incorporated as intended in the reference implementation. In cases where there is no way to test a particular requirement, a manufacturer must attest that they meet the criteria established in the specification.

The efficacy of developing requirements in this triad model (specification, reference implementation and certification) in concert becomes apparent when mapping the OCF specification to any of the several recent IoT security baseline requirements[1] developed by government and industry organizations, including NIST's own 8259D IoT security baseline.

These baseline mappings give manufacturers, consumers, and industry as a whole, compelling tools with which to measure and provide external validation of IoT security models and specifications. Should gaps become apparent between a given national baseline spec and the OCF specification, the OCF triad model allows the spec, reference code and certification test can be updated quickly, and in parallel, to close the gap and assure that compliance with OCF also means compliance with a given national security baseline.

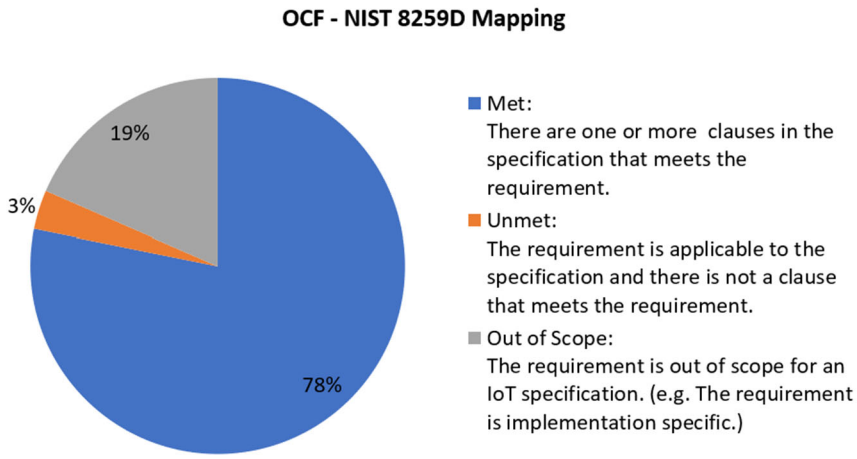

Figure 1: NIST 8259D Requirements met by OCF

Call to Action

Industry has already provided the specifications, conformance tests and open-source code necessary to jumpstart a national consumer software cybersecurity labeling program and these should be leveraged by NIST. OCF has gone a step further to ensure their ISO/IEC specs, code and compliance programs align with national schemes very close to the time of the scheme's publication. Working with OCF provides the US government the opportunity to leverage the OCF's responsive and concurrent specification, code, and certification process to see devices meeting the US IoT security consumer label requirements come to market almost immediately after publication, dramatically reducing NIST's timeline.

[1] https://openconnectivity.org/technology/ocf-security/