Labeling Consumer Products to Address Cybersecurity
Cisco Response to NIST Call for Papers
Cybersecurity Labeling for the Internet of Things (IoT) Devices and Consumer Software
August 17, 2021

Contact: Eliot Lear
Email: lear@cisco.com

The President's Executive Order (EO) on "Improving the Nation's Cybersecurity (14028)" issued on May 12, 2021 directs the National Institute of Standards and Technology (NIST) to undertake a series of initiatives related to the security and integrity of the software supply chain with the aim of improving our nation's cybersecurity—these include a direction for NIST to initiate two consumer labeling programs related to: 1) Internet of Things (IoT) devices; and 2) software security. Cisco Systems is pleased to provide NIST with a response to your call for submissions regarding consumer software labeling. As noted below, we believe this topic is inextricably linked with IoT security. Accordingly, we will address them together. Similarly, the line between consumers and enterprises has blurred, as many enterprise employees are now working from home or are in hybrid situations. As such, a consumer choice may well impact enterprise operations. We look forward to the opportunity to participate in the forthcoming workshop on September 14-15 concerning IoT baseline security criteria.

Broadly, we believe that the common theme across these two problem sets is whether and how consumer labels will foster demand for better security in devices that rely upon software. Much of the software that consumers purchase and use for connected devices is consumed via application stores or marketplaces that are already well-tended. Therefore, we recommend scoping those out of the current focus of NIST's work—except in-so-far as they provide an example of functioning marketplace. We also believe that the market for software purchased for computers for installation post-purchase should be set aside for the time being. Rather, we believe that the emerging area of risk where NIST's efforts can be most effectively focused is on software embedded or otherwise incorporated with devices, such as IoT devices in the consumer environment that interact with the physical environment. We believe there are several principles that should be applied to any software labeling standard for these consumer-oriented cyber-physical systems, which are discussed below.

Provide meaningful value

The labeling standard should provide meaningful value. Meaningful value in this case means that the label must be tied to practices that provide sufficient protection such that consumers need not worry that the software or device would become a threat to them or their neighbors.

Previous research has shown that a label alone can provide a false sense of security to consumers, leading to a reduced security posture when the consumer is led to believe that a standard provided protection, when fact it did not.[1] To avoid this situation, consumer product providers alone should not set standards for such labels. Research has also shown that it is important to give people meaningful choices.[2,3] That is, if there is any granularity to a labeling standard above a binary choice, it should be possible for the overwhelming majority of consumers to make a correct choice. We are skeptical that more choice will be meaningful to people not versed in cybersecurity.

[1] Adelman, B., Adverse Selection in Online "Trust" Certifications, Harvard Univeristy, 2006. https://www.benedelman.org/publications/advsel-trust-draft.pdf

[2] Sasse, M.A., Brostoff, S. & Weirich, D. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* **19,** 122–131 (2001). https://doi.org/10.1023/A:1011902718709

[3] M. A. Sasse and C. C. Palmer, "Protecting You [Guest editors' introduction]," in *IEEE Security & Privacy*, vol. 12, no. 1, pp. 11-13, Jan.-Feb. 2014, doi: 10.1109/MSP.2014.11.

Address evolving threats

Because the threat evolves, the standard attached to the label must also evolve. As NIST is aware, for instance, at some point the industry will need to be prepared for a post-quantum world. The norms for what is required will change, and consumer suppliers must react not only with their new offerings, but with their existing ones as well. Some means is necessary to communicate to consumers whether a device is still capable of a certain level of defense on an ongoing basis.

Enable expert defense

Consumers should not be expected to be IoT security experts, nor should they be expected to review labels and certifications on an ongoing basis. They may not even know what products are in their homes. This will especially be the case over time as people move into IoT-enabled or "smart" homes. The tooling should be in a position to discover which devices in the consumer environment have become vulnerable, so that they may assist the consumer in remediating any risks.

Firewall developers and Internet Service Providers have a meaningful role to play in providing that ongoing protection. NIST's focus should be on enabling access to the information that those organizations need. NIST can benefit from the views of the RIPE Labs, in which the consumer market is discussed.[4]

We recommend digital labels

A digital label is a set of claims that can be received and processed by automation. It should be signed by someone who has certified the product as having met a standard. It may be renewable. It may contain information about whether a product continues to be certified. In addition, a product supplier can apply a new digital label, should a product be qualified for additional certification. The label can indicate when a product is outdated and should be replaced. The label can also indicate other information, such as what sort of network protections the product needs, and what sort of vulnerabilities it may have.

Most importantly, digital information in standardized, machine-readable formats can enable intelligent, intuitive network services to automatically identify, provision, and protect devices by enabling only those permissions necessary for the device to operate as intended by the device manufacturer, the purchaser, and the network operator. Digital labels can be built on previous work of the National Cybersecurity Centers of Excellence (NCCoE) such as NIST SP 1800-15, and existing standards such as Manufacturer Usage Descriptions (MUD) [RFC 8520]. MUD provides a framework for information exchange about a device that can easily be extended to include certifications that can include software bills of materials and how to find security advisory information.

Labels won't fix everything

Labels and consumer education can only be effective insofar as they communicate information in terms reasonably likely to be understood and to purchasers who can be incentivized to respond accordingly. The Mirai botnet attack demonstrates the limits of this approach in that the devices that were exploited in a way that did not harm their owners, nor that their owners would even perceive. A rational, meaningful, commonly accepted baseline security standard should be introduced to undergird any consumer labeling program to facilitate effective protection of critical systems from connected IoT devices.

[4] https://www.ripe.net/publications/docs/ripe-759