From: Art Manion <amanion@cert.org>
Sent: Sunday, October 17, 2021 11:05 PM
To: EO-pilots
Cc: cert@cert.org; Laurie A Tyzenhaus
Subject: CERT/CC comments on DRAFT Baseline Security Criteria for Consumer IoT Devices

Dear NIST folks,

Please see the following comments on the August 31, 2021 DRAFT Baseline Security Criteria for
Consumer IoT Devices paper.

1. Scope of Labeling Criteria

In general, we suggest that labeling criteria apply to the combination of the manufacturer and the
device (not just the device, but the system that includes the device, often web services and mobile apps
and other devices).

Given the variety (in computing power, storage, cost, expected lifespan, rate of change, safety impact,
just to list a few) of IoT devices and systems, it will be difficult to identify technical capabilities that can
be applied universally. Furthermore, while technical capabilities may (do?) improve cybersecurity, no
collection of technical capabilities have yet produced a device or system that is free from latent
vulnerabilities. That is, manufacturer capabilities and practices are *required* to manage and maintain
security, regardless of technical capabilities.

A label based solely on device or system technical capabilities may not be effective. In effect,
manufacturer capabilities (Table 2) are more important than device capabilities (Table 1). In an extreme
view, manufacturers should receive labels, not products.

What can receive a label? The combination of a manufacturer performing appropriate non-technical
supporting capabilities for a specific device (system really) that supports appropriate technical
capabilities. The same manufacturer may offer un-labeled devices/ sytems. A device/system out of
support loses it's label, since the non-technical supporting capabilities are no longer in place.

2. Software Update

We are strong advocates of robust, reliable, secure software update capabilities. As noted in our comment #1, a device/system of course needs technical capability, but that capability is meaningless unless the manufacturer identifies vulnerabilities and delivers fixes. The manufacturer's capability is somewhat covered in Information Dissemination, but in our opinion not sufficiently. There should be a clear and distinct manufacturer capability to deliver updates.

As we understand it, the scope of this labeling effort is truly "consumer" oriented IoT. Consumers cannot be expected to read vendor security documentation and install security updates manually. For consumer products, the manufacturer (or service provider) essentially needs to push updates when needed, nearly silently and automatically (fine to give consumers choice about if and when to update, but the default workflow should be that security updates are nearly silent and automatic).

Do not expect to educate end-users much (in this case, about how and when to update devices), security capabilities must be largely handled by manufacturers and providers. The "walled garden" or "extended lease" models of software and system licenses are not without serious concerns, however they can provide security for large scale non-sophisticated groups. Perhaps a better model is manufacturer/provider control by default, users can individually opt out and manage their own device security (in this case, update), transferring more responsibility from the manufacturer/provider to the user.

For non-consumer IoT, where users have greater technical capability (e.g., ICS/OT, medical devices, other production and safety-critical systems), users and operators must be in control of updates.

To the extent possible, security updates should be independent of new features and breaking changes.

Centralized software update mechanisms also centralize risk and make attractive targets (M.E. Doc, Asus, SolarWinds). Guidance for software update capability must include consideration for this centralization of risk. Such risk might be mitigated by some sort of compartmentalization, so that the compromise of update infrastructure only affects a portion of devices/

systems.

3. Asset Identification

The current text does not specify globally unique identification, however, "a unique logical identifier" is open to such an interpretation. While necessary for network protocols and intentional device and user authentication -- intentionally authorized and consented to by the user -- identifiers pose significant privacy concerns. Such consideration should be provided as part of the guidance to have identifiers.

The current text says "... can inventory all of the IoT productís components." How can this be done by logical and physical identifiers? This "inventory" language seem to align more closely "All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component).

4. Documentation: Inventory

Speaking of the capability to document and provide "All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component)" -- while this is perhaps something less than baseline SBOM, it is unlikely any manufacturer will be able to product this documentation without obtaining SBOM information from their upstream manufacturers and suppliers. The manufacturer has to sort out the relationships in the supply chains in order to produce accurate inventory documentation. This is all that baseline SBOM purports to do.

5. Cybersecurity State Awareness

A fine idea, and it makes sense for devices and systems to log security events, maintain log integrity, and (perhaps less importantly) control access to logs. This capability stretches into logical unsatisfiability. How exactly does a computer or program know when it is operating incorrectly, has been attacked? If an adversary has control over the device or system, the adversary likely controls logging and owns system integrity. In light of our comment #6, perhaps reduce this capability to "log security events."

6. Simplicity

In general, labeling criteria and capabilities should be as simple as possible to meet some initial goal --
perhaps selecting a small number of capabilities with strong evidence that they improve security, that
can be observed/measured, and that the resulting labels can be understood by non-sophisticated
consumers. While we appreciate all of the capabilities in the draft paper, there are likely too many,
especially with a goal of end-user comprehension.

Here is a horribly rough idea for a simple label/criteria:

A. Manufacturer security support
Vulnerability management/CVD/VDP, SBOM/inventory, duration of security support, secure updates

B. Device/system security features
Reasonably new/fresh components and protocols (maybe SBOM/inventory here?), cryptography, attack
surface

C. Privacy
User data and sharing of user/device identity

Regards,

Art Manion and Laurie Tyzenhaus, CERT/CC