White Paper Draft- Baseline Security Criteria for Consumer IoT Devices

We reviewed this NIST Draft and appreciate this effort and the opportunity to provide the below comments from our SMEs for your consideration:

General comments

Intro, paragraph 2 – Much of the documentation is very vague about how IoT labelling will be implemented and who should implement it, even possibly having several possible different implementations. It may be good to identify groups who are the target implementers (maybe manufacturer alliances, standards groups) and recommendations for how to de-conflict conflicting implementations. An IoT labelling systems is not going to do consumers much good if there are 10+ different versions all implemented and scored differently.

Response to NIST highlighted specific areas for consideration:

o Whether these are appropriate criteria for a broad range of consumer devices

Yes, these seem appropriate for a broad range of consumer devices. I went through the criteria for several different sectors of IoT and saw no glaring issues or types of devices that wouldn't be able to conform to a majority of the criteria if the manufacturer wished to do so.

o Whether additional criteria are needed, including criteria that specifically address other components of the product beyond the device

I think the biggest challenge with this effort is how to handle the supporting IoT ecosystem associated with the devices. The cloud backend, mobile apps, device integrations with other IoT systems, etc. play a huge part of IoT cybersecurity and these components will likely change frequently due to product updates, company mergers and buyouts, etc.. There wasn't much in the criteria dedicated to the backend aspects of IoT and that is probably something that should be expanded on.

o Whether Tables 1, 2, and 3 have the right level of detail in the discussion of the criteria to ensure consistency in meeting the cybersecurity expectations

Yes, the tables seem to have the appropriate level of detail and NISTIR 8259A is available for reference if further clarification is needed.

o The extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria

There are definitely several categories of criteria from tables 1 and 2 that would apply to microcontrollers. These limited devices should still go through the labeling exercise and implement applicable criteria, but not be penalized for criteria that cannot be met due to device limitations. I had an initial thought of making a subset of the criteria for microcontrollers, but that could vary greatly depending on the device and it would likely not be a feasible exercise.

o The potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another

This will be a huge challenge due to the scope of these components and how frequently they change, but they are a critical component of the IoT device's cybersecurity and this is absolutely something that needs to happen.

Table 1 Comments

Asset identification - Logical identifier and physical identifier could use more clarification (even in the reference document NISTIR 8259A). Are the identifiers unique per device or per make and model? How will manufacturers ensure that there are no identifier conflicts?

Data protection –

#1 – May want to add that the cryptographic algorithms should be implemented from trusted, well-vetted libraries/modules and not "home grown"

#3 - it is not clear what is being said here. Is the intent to keep all configuration data and software blocked for all but authorized users? This probably just needs to be re-worded.

Logical Access to Interfaces –

#5 – an option to connect to a centrally managed authentication service (e.g., Active Directory) would be a good thing to add

Software Update –

#3 – It doesn't seem like a good security measure to disable notifications about updates

Cybersecurity State Awareness –

#3 – possibly update to include verifying that there have been no unauthorized edits of state information through the use of cryptographic hashes and other security measures

Table 2 Comments

Documentation – Add in a criterion that all documentation be updated whenever there are changes to the product, cloud backend, app, etc..

> General comment – some of the items asked for in #1 – 8 seem very sensitive and many companies would likely balk at providing these details.

Information and Query Reception

#1 – this should include a method for customers to self-identify/subscribe to these updates to support second-hand purchases

Table 3 Comments

Is the intent to keep table 3 as a separate set of criteria, or is this just included to highlight potential changes to table 1? The tables should be merged if possible as table 3 continues to add to an already overwhelming list of criteria, especially to the average consumer who will have likely already been overwhelmed by these requirements.

Under Increasingly Comprehensive Levels of Testing and Assessment (Tiers) on page ten after last sentence of last paragraph recommend leverage ideas for IOT labels from other existing successful label programs such as energy star label approved by Department of Energy (DOE) and already accepted by consumers as being a reliable label source to help them decide on purchasing the most energy efficient products. Energy Star is the government backed symbol for energy efficiency and was introduced as a volunteer labeling program to identify and promote energy efficient products. Similar IOT label program can help consumers identify security levels of products and incentivize companies to achieve these goals to meet consumer demand for more secure products.

Under Criteria for the Label after the last sentence on page eleven recommend adding that

Since the label is intended to communicate compliance with a set 11 of cybersecurity criteria, suggest that there also be a government approved graphic in the label similar to Energy Star Label approved by the government to help inform consumers on energy efficiency levels and incentivize companies to comply with the goals. Recommend work towards goal of similar graphic used in energy star label that is easily recognized as a government approved product and Section 508 compliant for electronic versions, since it is important that consumer IoT product cybersecurity labels are understandable by all the consumers in order to be effective and actionable for IOT security: