RED ALERT LABS
IoT Security

Red Alert Labs

Comments on "Draft IoT Device Labeling Criteria"

Summary of draft NIST white paper

Red Alert Labs congratulates NIST on the draft white paper "IoT Device Labeling Criteria", prepared in response to Executive Order (EO) 14028, "Improving the Nation's Cybersecurity". Section 4 (t) of the EO states

> Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

In the first paragraph of the white paper, NIST states that

> This white paper proposes baseline security criteria for consumer IoT devices. This is one of three dimensions of a consumer Internet of Things (IoT) cybersecurity labeling program that would be responsive to Sections 4 (s) and (t) of the EO. The other dimensions are criteria for conformity assessment and the label.

The following are the primary elements of the device labeling program described in the white paper:

1. NIST started with the "capabilities described in NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline and NISTIR 8259B, IoT Non-Technical Supporting Capability Core Baseline". NIST points out, "These are core baselines and need to be tailored (or profiled) for specific use cases or sectors."
2. "Through a review of the landscape of related informative references from governments, non-profit, and private sector sources", NIST then developed a "profile" of those baselines.
3. NIST selected "technical criteria for extending or editing the baseline", based on three considerations:
    a. Utility for cybersecurity;
    b. Feasibility of implementation; and
    c. Support for labeling and conformity assessment.

NIST's six questions

NIST continues,

> "NIST seeks comment on all aspects of cybersecurity labeling technical criteria for IoT devices. Specific areas for consideration include:
>
> - Whether these are appropriate criteria for a broad range of consumer devices
> - Whether additional criteria are needed, including criteria that specifically address other components of the product beyond the device
> - 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
> - What might be the appropriate definitive text for these criteria be stated to facilitate conformity assessment
> - The extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria
> - The potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another"

In these comments, Red Alert Labs (RAL) will answer each of these questions to the best of our knowledge. We will also provide suggestions on how NIST might enhance the device labeling program, in order to address product-specific threats not addressed by the current criteria.

1. Are these appropriate criteria for a broad range of consumer devices?

RAL believes that all of the criteria selected by NIST are appropriate and applicable to a broad range of consumer devices. In Table 1 and Table 3, NIST lists Potential Criteria that are applicable to the items listed under the six categories of Device Cybersecurity Capabilities from NISTIR 8259A: Asset Identification, Product Configuration, Data Protection[1], Logical Access to Interfaces, Software Update, and Cybersecurity State Awareness. To these, NIST adds a seventh Device Cybersecurity Capability: Product Security.

For each of these Capabilities, NIST selects Potential Criteria that are likely to be appropriate for a broad range of IoT product types. For example, the Potential Criteria for the Asset Identification Capability are:

1. A unique logical identifier, possibly generated by the product component host; and
2. A unique physical identifier at an external or internal location on the device accessible to the consumer.

Similarly, in Table 2, NIST lists Potential Criteria that are applicable to the items listed under the four categories of Non-Technical Supporting Capabilities found in NISTIR 8259B: Documentation, Information and Query Reception, Information Dissemination, and Education and Awareness. Again, the Potential Criteria selected by NIST are likely to be appropriate for a broad range of IoT product types. For example, the Potential Criteria for the Information and Query Reception Non-Technical Supporting Capability are:

[1] In describing this category, NIST noted that "available cryptographic modules may be dependent on or limited by the product component host."

1. The ability for the manufacturer and/or supporting entity to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from their customers and others in the IoT product ecosystem.
2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party (e.g., repair technical acting on behalf of the consumer) queries about cybersecurity of the IoT product and its components (e.g., customer support).

RAL believes that all of the Potential Criteria listed in Tables 1 and 2 are appropriate to include in the IoT device labeling program.

2. Are additional criteria needed, including criteria that specifically address other components of the product beyond the device?

In Table 3, NIST identifies "Potential Additional Criteria" for each of the seven Device Cybersecurity Capabilities listed in Table 1. Each of these sets of additional criteria addresses "other components of the product beyond the device" – for example, the cloud component. RAL believes that these Potential Additional Criteria would all be appropriate to include in the IoT device labeling program.

There might well be additional criteria that could be assessed specifically for the cloud backend and mobile app components, e.g. regarding authentication to or secure deployment of those components. See our answer to question 6 below for further discussion of this idea.

3. Do 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. Red Alert Labs believes that the tables provide the right level of detail, without providing overly prescriptive requirements. For the sake of clarity, we suggest that the examples provided in the text be clearly separated from the criteria definition. They could be tagged as "application note" or "example".

4. What might be the appropriate definitive text for these criteria, to facilitate conformity assessment?

The appropriate definitive text for each of the criteria, to facilitate conformity assessment, will vary by the criterion. In general, the criteria should be rephrased as requirements, although not prescriptive ones. For example:

1. Under the "Product Configuration" IoT Product Cybersecurity Capability on page 3 (Table 1), the second Potential Criteria is "The ability to restrict configuration changes to authorized individuals and other IoT product components only." To facilitate conformity assessment, RAL recommends that this be reworded to "The capability to make configuration changes should be restricted to authorized individuals and other IoT product components only."
2. Under the "Software Update" IoT Product Cybersecurity Capability on page 4 (Table 1), the first Potential Criteria is "The ability to update the product component's software through remote (e.g., network download)." We recommend that this be reworded to "The product should be capable of updating its software through remote access (e.g. network download)."
3. Under the "Information and Query Reception" Non-Technical Supporting Capability on page 7 (Table 2), the first Potential Criteria is "The ability for the manufacturer and/or supporting entity

to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from their customers and others in the IoT product ecosystem." RAL recommends that this be reworded to "The manufacturer and/or supporting entity should identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from their customers and others in the IoT product ecosystem."

5. To what extent can consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) address the criteria?

It is certainly true that some of the criteria will not be addressable using IoT devices with very limited capabilities. However, this in itself isn't necessarily a problem, since the device's failure to address a particular criterion might not in itself create an unacceptable risk, depending on the type of device or the environment in which it will be deployed. For example:

1. The single criterion for "Product Security" in Table 1 starts with "The ability for the device to continue operating (possibly with limited digital functionality) in the case of a network outage or other connectivity disruption." For devices like smart refrigerators, this ability is obviously essential to achieving the purpose of the device; a refrigerator that couldn't keep food cold during a network outage would be worse than worthless, since it might endanger the health of the occupants of the household. On the other hand, for a video doorbell, the fact that the camera might not function in the event of a connectivity disruption would probably not be considered an unacceptable risk, as long as the visitor can make their presence known by knocking or ringing a "dumb" doorbell.
2. One of the criteria for "Logical Access to Interfaces" in Table 1 is "The ability of the product component to validate that the input received through its interfaces matches specified definitions of format and content." In many commercial and industrial uses, this would be a critical capability. In fact, not having it might make the device unusable in those environments. However, for home or small business uses, not having this capability might in many cases be acceptable, if it would help keep the cost down.

6. What is the potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another?

This is a good question. The answer to it is "It varies by the component." Assessing the cloud backend – and doing a thorough job of it – might be expensive, since it requires learning about the cloud provider's security practices, or at the least obtaining the results of its most recent FedRAMP or SOC II audit. It also requires learning about the security controls that the IoT device manufacturer has put in place for their environment in the cloud. This is because major cloud providers like AWS and Microsoft Azure require the customer to be responsible for most of their own security, unless they want to pay extra to have the provider be responsible. The EU Cloud Service Certification Scheme that is currently being finalized in Europe by ENISA will tell us more in the upcoming few years about the efficiency of such certification for assessing the IoT Cloud Services/Platforms, for instance.

The hub should be assessable, and since one hub might be used for multiple manufacturers' IoT products, the results might be reusable for an assessment of a different product that uses the same version of the same hub.

The mobile app is also independently assessable, and assessing it is important in its own right – for example, how the user authenticates to the mobile app is a very important question. In fact, it's certainly possible that some of the most significant vulnerabilities of an IoT product (including the device and the other components) would come through the mobile app, not the device itself. So the app should be assessed separately, if at all possible. In fact, this might fall under the consumer software labeling program, not the IoT device labeling program.

In general, the assessment of any IoT product component should provide the level of assurance based on a holistic risk analysis that takes account of any potential cybersecurity threat that could occur on the whole IoT value chain (from chip to cloud). Therefore, any component should be independently assessable, as long as the assessment considers the intended use (assumptions, policies, … applicable to other components) in the risk analysis.

Other desirable criteria

As discussed above, RAL believes that all of the criteria listed in the white paper are appropriate to include in the IoT device cybersecurity labeling program. All of these are basic capabilities that are appropriate to almost any IoT product. They all are responses to fundamental threats faced by most IoT products.

However, it is well known that there is a huge variety of IoT product types, and there are a huge number of threats that apply only to one or a few product types. It would be worthwhile to include – in some way - criteria that address these limited-applicability threats, such as the following criteria from ETSI EN 303 645:

- **Provision 5.1-5** When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.
- **Provision 5.3-7** The device shall use best practice cryptography to facilitate secure update mechanisms.
- **Provision 5.5-4** Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.
- **Provision 5.5-6** Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.
- **Provision 5.13-1** The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

Implementing these provisions in an IoT device will sometimes make it uncompetitive in its market – for example, a baby monitor or a smart refrigerator. However, in other types of devices, especially those used in businesses or government agencies, some or all of these provisions might be very appropriate.

However, the answer isn't simply to throw every possible criterion into the program. Since so many of these apply only to a small number of IoT device types, trying to include all criteria in one program would be very confusing and unwieldy.

It might be suggested that additional criteria be included that apply to particular device types – so there could be separate sets of criteria for security cameras, smart washing machines, remote terminal units, network switches, etc. However, deciding on these separate criteria would require a huge amount of work by experts from widely different disciplines; it would also likely be very contentious. How can the IoT device cybersecurity labeling program address product-specific cyber threats, without having to go through this process?

The Finnish example

In 2019, Finland's National Cyber Security Centre (NCSC) and Traficom, the Finnish Transport and Communications Agency, introduced an IoT device cybersecurity labeling program that might point the way toward the solution to this problem. In order to receive the label, the device must be assessed in three ways:

1. The device and manufacturer must meet 18 of the 68 ETSI 303 645 provisions. Like the criteria shown in Tables 1-3 of the NIST white paper, these 18 provisions are likely to apply to the great majority of IoT devices, so it is appropriate that almost all devices are required to meet them.
2. Threat modeling must be performed against the product. This identifies the most important threats that are applicable to that product. They will be specific to the type of product, how it will be deployed, the intended customers, etc.
3. The threats that are identified through threat modeling must be tested. If the product does not currently address one or more of those threats, they must be mitigated before the product will receive the label.

Red Alert Labs suggests that NIST consider adding threat modeling as another component of the IoT device labeling program, along with meeting the criteria already identified. We believe this is the best way to address serious threats that apply only to a small number of devices, as well as the basic threats that apply to almost all devices. The product would need to be tested for protections against the threats identified by the threat modeling.

However, it isn't necessary that all devices – or perhaps even the majority of devices – be required to undertake threat modeling. For many IoT products, especially those used exclusively in the home, the criteria that NIST has already identified will address all of the important threats that are applicable to the product. However, NIST should require threat modeling for certain categories of products, such as

- Products that store or transmit sensitive data that must be protected;
- Products whose misuse or compromise might lead to physical damage or harm to individuals; or
- Devices that might be installed on business, government or military networks, where a compromise could harm other important systems or data.

Conclusion

Red Alert Labs believes the IoT device cybersecurity labeling criteria identified by NIST are sufficient to assess important cyber threats applicable to the majority of IoT products. However, for products that fall in specific categories like the ones above, we believe it would be a good idea to consider requiring threat modeling, along with testing of whether or not the product has addressed the threats identified in the threat model. Products that fail one or more of these tests will need to fix the problems and be re-tested, in order to receive the label.

Roland Atoui, Red Alert Labs, roland.atoui@redalertlabs.com
Tom Alrich, Red Alert Labs, tom.alrich@redalertlabs.com