Securing IoT Devices (Part 2): Inside the NIST Guidance Document for IoT Device Manufacturers

August 22, 2019

At the end of July, the National Institute for Standards and Technology ("NIST") released draft cybersecurity guidance for IoT device manufacturers. The document, titled *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*, is intended, according to NIST, identify the cybersecurity features that IoT devices should have "to make them at least minimally securable by the individuals and organizations who acquire and use them." The NIST document is not a rule or requirement for IoT devices, but rather is a continuation of NIST's effort to foster the development and application of voluntary standards, guidelines, and related tools to improve the cybersecurity of connected devices.

NIST is seeking comment on the document through September 30 of this year and it held a workshop in August for interested parties to discuss the document. In a prior post, I blogged on takeaways from that workshop. Now, it's time to take a closer look at the NIST document itself.

Overview of the Baseline

The NIST Baseline ("NISTIR 8259" in government-speak) is subtitled "A Starting Point for IoT Device Manufacturers," and it is intended as just that. NISTIR 8259 builds upon a base document released in final form on June 27, 2019 relating to cybersecurity and privacy risks for the Internet of Things. IoT manufacturers should review NIST's *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* before digging into the Baseline document. *Considerations* (also known as NISTIR 8228) identifies high-level considerations that make IoT security different than IT security and offers suggestions for mitigating cybersecurity and privacy risks. Its intended audience primarily are the users and organizations deploying IoT devices, but it has meaning for manufacturers, network operators and service providers in the space as well.

The NIST Baseline takes these considerations to the manufacturing side, offering (as NIST describes it) to help IoT device manufacturers "understand the cybersecurity risks their customers face" so IoT devices can provide the minimal features to make them securable. (For a discussion of the different meanings that "securable devices" can have in this context, see my blog post on the NIST workshop.)

Securing IoT Devices

The NIST Baseline explains that cybersecurity risks for IoT devices have two high-level risk mitigation goals: protecting device security and protecting data security. As noted in the user-focused *Considerations* document, the challenges in doing so stem from three features of the Internet of Things:

1. IoT devices interact with the physical world in ways conventional IT devices usually do not. (In other words, they are, by their nature, connected devices.);

2. Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can; and

3. The availability, efficiency, and effectiveness of cybersecurity features are often different for IoT devices than conventional IT devices.

The NIST Baseline focuses on a *generic* customer to define the "core" baseline features. The draft notes that manufacturers may need to identify and implement additional features beyond the core baseline that are most appropriate for customers of their particular devices and applications, and offers information on how manufacturers can do this.

For the "core," NIST identifies six features that IoT devices should address:

1. **Device Identification.** How the IoT device can be uniquely identified, both logically and physically.

2. **Device Configuration.** How the device's software and firmware can be changed and who is authorized to make such changes.

3. **Data Protection.** How the device can protect from unauthorized access and modification the data that it stores and transmits.

4. **Logical Access to Interfaces.** How the device can limit (logical) access to its local and network interfaces so that only authorized users may access these elements.

5. **Software and Firmware Updates.** How the device can be updated by authorized entities only, using a secure and configurable mechanism.

6. **Cybersecurity Event Logging.** How the device can log cybersecurity events and make the logs accessible to authorized entities only.

For each core feature, the NIST Baseline identifies, in table form, the key elements to consider, the rationale for the feature and several reference documents that may be helpful in addressing the feature. In keeping with NIST's limited role, the Baseline focuses on the "what" that needs to be addressed, not on the "how" manufacturers should address it.

Separate from the core features, the NIST Baseline also discusses two areas relevant to securing IoT devices. First, it discusses considerations for implementation of these features in the design and manufacturing process. Second, it discusses considerations in communicating these features and the cybersecurity risks of IoT devices to the manufacturer's customers and users of the device (users who may not necessarily have been the ones to purchase or configure the device).

Issues for Comment

Unlike FCC or FTC notices seeking comment, the NIST Baseline does not provide specific questions or issues for comment. Instead, the Baseline simply seeks feedback from all stakeholders on the draft, in order to assist NIST in refining the document.

The NIST workshop that I attended offers some insight into the comment areas that NIST would find helpful. In the discussion group sessions, NIST first asked whether the six core features were

sufficient, and whether any other considerations should be added to the list. My group spent a lot of time discussing the relationship between the Baseline and efforts to create industry-specific standards or best practices. NIST seemed very interested in determining whether the Baseline would serve as a useful starting point for those efforts.

Second, the discussion group was asked whether customer communication should be a core feature or a separate consideration (as in the draft now). This seemed to focus on the role that shared responsibility among manufacturers, users, control organizations (like a corporate IT group) and/or the government played in securing devices (or making them securable).

Finally, our discussion group was asked about two potential additions to the Baseline. First, we were asked whether considerations in protecting legacy devices in an IoT network should be added. This question raised the issue of the role a single IoT device plays in a larger network, such as a smart home configuration where multiple devices (potentially from multiple manufacturers) are controlled by a central hub device. Second, we were asked whether exterior threats to the devices, such a DDoS attack or botnet attacks, should be part of the Baseline.

Any and all of the above should be fair game for comment to NIST on the Baseline. Comments on the NIST draft may be submitted through September 30. Kelley Drye is working with device manufacturers on potential comments to NIST. If you are interested in submitting comments, please feel free to contact us.