NIST Releases Draft Security Feature Recommendations for IoT Devices

Submitted by willirn1 on Thu, 09/26/2019 - 11:29am

NIST Releases Draft Security Feature Recommendations for IoT Devices

"Core Baseline" guide offers practical advice for using everyday items that link to computer networks.

August 01, 2019

Appliances from refrigerators to thermostats are now available in models that interact with a wireless network, making them easier to control with a computer or smartphone. Because these devices can also put our security at risk, the National Institute of Standards and Technology (NIST) has released a guide to help us all adjust to a world where seemingly everything is connected -- and potentially vulnerable.

The guide identifies a set of voluntary recommended cybersecurity features to include in network-capable devices, whether designed for the home, the hospital or the factory floor. Although the guide's subtitle is A Starting Point for IoT Device Manufacturers, its principles can be useful to anyone who links a device to the internet.

"This 'Core Baseline' guide offers some recommendations for what an IoT device should do and what security features it should possess," said Mike Fagan, a NIST computer scientist and one of the guide's authors. "It is aimed at a technical audience, but we hope to help consumers as well as manufacturers."

As with a number of other NIST cybersecurity publications, the Core Baseline, whose full title is Core Cybersecurity Feature Baseline for Securable IoT Devices (Draft NISTIR 8259), is not a set of rules for manufacturers to follow. Rather, it is voluntary guidance intended to help promote the best available practices for mitigating risks to IoT security. It complements the recent publication of Considerations for Managing Internet of Things Cybersecurity and Privacy Risks (NISTIR 8228), which primarily addresses large organizations that have more resources to dedicate to IoT cybersecurity.

IoT devices can provide tremendous benefits (e.g., smart medical devices) as well as a host of conveniences, like checking our refrigerator's contents from the grocery store. They also create a new type of cybersecurity risk for a society that already suffers newsworthy hacks and data breaches on a regular basis. While a conventional computer might require a password entered from a keyboard, a network-capable coffee maker might have no keyboard at all -- but would still appear on a home or office wireless network. This and countless other small electronic devices could be vulnerable to hacking if they do not possess security features that an owner understands and uses.

"Securing devices is a group effort," Fagan said. "The manufacturer has to supply options and software updates, and the user has to apply them. Both sides have roles to play."

The Core Baseline provides a list of six recommended security features that manufacturers can build into IoT devices, and that consumers can look for on a device's box or online description while shopping. While the document includes technical language not intended for consumers, Fagan provided a straightforward explanation of each feature:

- Device Identification: The IoT device should have a way to identify itself, such as a serial number and/or a unique address used when connecting to networks.
- Device Configuration: Similarly, an authorized user should be able to change the device's software and firmware configuration. For example, many IoT devices have a way to change their functionality or manage security features.
- Data Protection: It should be clear how the IoT device protects the data that it stores and sends over the network from unauthorized access and modification. For example, some devices use encryption to obscure the data held on the internal storage of the device.
- Logical Access to Interfaces: The device should limit access to its local and network interfaces. For example, the IoT device and its supporting software should gather and authenticate the identity of users attempting to access the device, such as through a username and password.
- Software and Firmware Update: A device's software and firmware should be updatable using a secure and configurable mechanism. For example, some IoT devices receive automatic updates from the manufacturer, requiring little to no work from the user.
- Cybersecurity Event Logging: IoT devices should log cybersecurity events and make the logs accessible to the owner or manufacturer. These logs can help users and developers identify vulnerabilities in devices to secure or fix them.

Fagan said that home users might appreciate the value of some of these features more easily -- particularly data protection, regular software updates, and interface access controls (which stop other people from accessing your device). Other features represent a more nuanced benefit, such as the ability to reset a device securely to its original settings if the device ever changes hands. All of the feature recommendations in the draft IoT Core Baseline were developed as part of a public/private partnership with industry, government and academic stakeholders.

To improve the Core Baseline further, NIST will hold a workshop on Aug. 13, 2019, to gather feedback on the draft. The authors will hold breakout sessions to discuss aspects of the draft with the stakeholder community. Registration is open until Aug. 6. The agency will accept public comments on the draft until Sept. 30, 2019, after which the authors will begin work refining the guide for a future edition.

For more information, visit: https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices

CPS Technologies Foundations Cybersecurity information technology Internet of Things (IoT) privacy 2019 NIST U.S. Government