Considerations for Managing IoT Cybersecurity and Privacy Risks Workshop Summary

What we heard and next steps

July 11, 2018 Workshop

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Background

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT can provide computing functionality and network connectivity for equipment that previously lacked these, as well as the ability to analyze data about the physical world and use the results to better inform decision-making, alter the physical environment, and anticipate future events. While the full scope of IoT is not precisely defined, it is clearly vast. Many organizations are not necessarily aware they are using a large number of IoT devices, which can affect their cybersecurity and privacy risks in different ways than traditional information technology (IT) devices. Once organizations are aware of their existing and possible future IoT usage, they can begin to understand how the characteristics of IoT affect managing cybersecurity and privacy risks.

The National Institute of Standards and Technology (NIST) Cybersecurity for IoT Program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the Program aims to cultivate trust and foster an environment that enables innovation on a global scale.

On July 11, 2018, NIST held a workshop in Gaithersburg, Maryland to further inform development of a publication on an introduction to considerations for managing IoT cybersecurity and privacy risk for federal agencies. NIST released a pre-read document in advance of the workshop to help guide discussions at the workshop. This document summarizes the most prevalent discussion themes from the workshop, and highlights NIST's next steps.

Opening Session

In his opening remarks, Kevin Stine, Chief of the Applied Cybersecurity Division in NIST's Information Technology Laboratory, touched upon the power and potential of the Internet of Things, as well as the need to consider not just current but also potential future cybersecurity and privacy challenges as the IoT landscape continues to grow. He described NIST's cybersecurity and privacy program, and reinforced the importance of the open, transparent, and collaborative approach NIST uses to develop and issue standards, guidelines, and tools to help organizations understand and manage cybersecurity risk. Leveraging NIST's longstanding cybersecurity and privacy program, and through significant engagements with diverse stakeholders over the last year, NIST began drafting a publication – an introduction to considerations for managing IoT cybersecurity and privacy risks for federal systems.

Fireside Chat

Katerina Megas, Program Manager for NIST's Cybersecurity for IoT Program, and Naomi Lefkovitz, Program Manager for NIST's Privacy Engineering Program, joined Kevin Stine for a fireside chat to lay the groundwork for the day's sessions. In this discussion, they explained why their programs are collaborating to draft the publication and what the desired objectives are to achieve at the workshop.

In response to stakeholder input that highlighted that IoT devices have a large range of capabilities and exist in an environment or an ecosystem, NIST is focusing this publication on helping the organizations that use IoT manage their risks. The desired objective of this workshop was to hear from industry to help inform NIST in writing this publication. This included getting feedback on:

- Identifying considerations for managing cybersecurity and privacy risk for IoT devices versus conventional IT devices;
- determining how those risks might impact risk management in general and risk response and mitigation in particular; and
- identifying basic cybersecurity and privacy controls organizations may want to consider, adapt, and potentially include in their requirements when acquiring IoT devices.

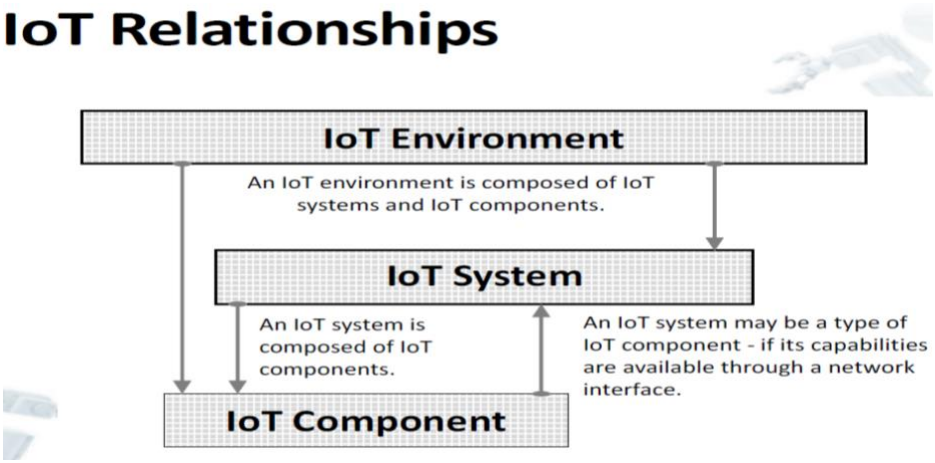
Stakeholder feedback has reinforced the importance of managing cybersecurity and privacy risks, including for IoT, in a coordinated manner. The integration of cybersecurity and privacy risk considerations in this publication reflects the broader approach NIST is taking to enable cybersecurity and privacy programs to understand and manage risk, produce trustworthy systems, leverage resources efficiently, and improve mission outcomes.

A Proposed IoT Model

Eric Simmon, a systems expert in NIST's Software and Systems Division, presented a proposed model for IoT. While there are a number of existing definitions, Mr. Simmon suggested there are two essential concepts for IoT:

- The capacity to support many-to-many networked relationships between components. These digital network capabilities may or may not be TCP/IP based, and the many-to-many relationship may or may not be used.
- The presence of sensors and/or actuators that allow the components to interact with the physical world.

The proposed model includes a description of the relationships between IoT components, IoT systems, and IoT environments.



Further, the proposed IoT model includes a set of capabilities to describe an IoT component, including transducer capabilities (actuating, sensing); data capabilities (transferring, processing, storing); interface capabilities (application interface, human user interface, network interface); supporting capabilities; and latent capabilities.

Working Session Summaries

The workshop agenda reflected topics of interest based on the aspects of cybersecurity and privacy risks where our initial analysis found the need for more information and discussion to be greatest. Generally, those topics addressed:

- Risk considerations for IoT;

- Applying IT cybersecurity controls to IoT;
- IoT baselines and overlays; and
- Identifying and managing privacy risks for IoT.

Frequent themes identified from the stakeholder feedback included:

- The need to consider the entire ecosystem, not just the device or the data;
- Challenges posed by legacy systems and the need to consider a device's lifecycle;
- Considerations particular to a specific industry or use case; and
- The need for a common language to discuss IoT cybersecurity and privacy risks.

The following sections summarize the working session discussions.

Breakout One: Risk Considerations for IoT

The proposed IoT model describes IoT capabilities. This session explored the cybersecurity and privacy risk considerations for these capabilities and the challenges in addressing them. One theme of the discussion was ways to classify IoT, including creating categories of devices, and determining risks specific to each category. However, there was no consensus on how devices should be categorized, such as by type, capability, or use case. Another theme was the role of the device itself. Some participants pointed out that different device capabilities – and combinations of capabilities – introduce a different set of risks. Capability inventories and controls assessments were discussed as possible risk mitigation approaches.

Participants also discussed the way the environment in which the device is deployed introduces or changes the relevant cybersecurity and privacy risks. Some noted that this is particularly important since IoT devices have different capabilities. Device lifecycle considerations were also mentioned: since many IoT devices are embedded or completely self-contained, it may be hard to replace specific IoT components or parts, a very different scenario from traditional IT. Participants also discussed the importance of visibility into a device's supply chain, as well as for consumers to know what functions are in use and enabled on a device.

Regarding an approach to IoT cybersecurity, participants agreed there is no "one size fits all" approach because devices, capabilities, environments, use cases, and mission needs vary so greatly. Some participants suggested that each organization is in the best position to specify the security controls for its IoT devices because needs and uses vary. Others were interested in identifying a common baseline of controls applicable to all IoT devices. Participants suggested that device- or use case-specific control overlays could be applied above the common baseline to further secure IoT devices and systems.

Breakout Two: Applying IT Cybersecurity Controls to IoT

In this breakout, participants discussed the challenges of applying IT cybersecurity controls to IoT devices, including whether all the traditional cybersecurity controls are needed and whether IT and IoT devices are too different to be secured in the same manner. Some suggested considering the capabilities and constraints of IoT devices, as these are what determines the level of risk associated with a device; further, knowledge of the environment or ecosystem will inform whether a particular device should be deployed there, depending on its capabilities and constraints. Participants discussed whether controls should change as the environment itself changes.

Identification, asset management, patching, and updating were also discussed as challenges to applying IT cybersecurity controls to IoT. Participants tended to agree that IoT devices should have an identifier, though there was no consensus on how this should be accomplished. Some noted that identification, software updates, and patching were particularly troublesome in industries such as healthcare, where hospitals may have challenges updating a life-preserving device such as a heart pacemaker and/or often have outside organizations manually do asset management just once a year. The complexities of IoT supply chain and third-party access control were also mentioned.

Participants indicated that physical security poses a challenge as users can't always assume IoT devices will be in a secure environment, and compensating controls may be needed to combat this. The widespread and diverse nature of IoT devices. IoT devices are often unattended in unsecure locations, meaning they may be prone or susceptible to tampering without detection. However, the scale of IoT may be a mitigating factor for physical security; it may be less worth a bad actor's time to tamper with a device because there are so many devices and most have little information of value to the bad actor.

Network segregation was discussed as a compensating control. However, participants noted it introduces its own set of challenges: if similar devices are collected on a network segment, then successful attacks against that segment could have access to a collection of similarly vulnerable devices. Whitelisting and analytics were discussed as possibilities to combat weaknesses with network segregation, but there was agreement that these approaches are still difficult.

Breakout Three: IoT Baselines and Overlays

Stakeholders have expressed a strong interest in cybersecurity and privacy baselines for IoT, such as minimum sets of NIST Special Publication (SP) 800-53 security and privacy controls or a set of capabilities that could be used for all IoT devices. This breakout session explored opportunities to create IoT baselines, as well as Cybersecurity Framework profiles and SP 800-53 overlays, and examined possible candidates for inclusion in baselines.

Participants were interested in NIST developing a set of recommendations and suggested using the Cybersecurity Framework, SP 800-53, and other existing references such as UL 2900 and ISO 62443. The level of specificity recommended by participants varied: while some participants supported a more prescriptive set of requirements, others wanted an approach or set of more general recommendations that could be applied as needed. They noted that the selection and implementation of cybersecurity and privacy controls should be based on the device's operating environment, its data, its use, and methods of access.

In addition, participants discussed the feasibility of having a single baseline for all IoT devices. While baselines could be useful, it was acknowledged that regulated sectors would each have different baselines based on its use and environment, and there was lack of consensus whether there can be a core set across all IoT devices. There was also recognition that legacy and non-legacy devices would require different security capabilities. Some participants acknowledged that they would like NIST to identify controls or capabilities that would apply to any IoT device, but a majority noted that it may not be feasible due to the variety in IoT devices.

Organizational missions and business objectives, requirements, and risk tolerances were discussed as important factors to inform development of baselines. Participants noted that different baselines and rulesets apply to different devices and operating environments, especially when considering legacy and

non-legacy devices, or when operating in sectors that have existing policy and regulatory structures in place. They emphasized that pre-market and post-market controls matter, and that flexibility is important as the technology matures.

Breakout Four: Identifying and Managing Privacy Risks for IoT

Privacy and cybersecurity overlap in areas such as protecting the confidentiality of PII, but there may also be privacy concerns not connected to cybersecurity. This breakout focused on how to identify and manage IoT-specific privacy risks. Overall, participants wanted NIST to develop guidelines for managing IoT cybersecurity and privacy risks. Regarding privacy, participants tended to agree that IoT guidance needs to include – at a minimum – discussions of: capabilities that help identify an IoT device; the data lifecycle and how to manage privacy risks throughout; and how to use post-market controls to manage risk.

Participants focused on the IoT ecosystem as a whole, and some proposed focusing on data as opposed to the device. Devices can be part of multiple ecosystems, with data moving between each of them. There was also discussion of what happens if any ecosystem components go offline; there could be a security risk and data could be released, thus affecting the device's overall cybersecurity and privacy. Further, some pointed out that location of data storage was not addressed in the pre-read. The location of where the data is being collected and transferred can determine the level of risk. Often, they noted, decentralization of the data and devices can impact the privacy risk.

There were also discussions surrounding whether manufacturers or consumers are responsible for implementing privacy controls. Some noted that manufacturers should communicate the capabilities and risk of their IoT devices as the manufacturers are in the best position to inform the customers of their product and potential privacy risks, as well as the built-in capabilities to mitigate these risks. However, others argued that manufacturers don't know what the device will be used for, nor can they predict all the ways the device will be used, so they shouldn't be responsible for implementing or enabling privacy controls or features. Instead, some suggested manufacturers can only meet privacy requirements for the intended operation of the product. One thought was that every time an IoT system changed ownership, there should be a statement of expected operation and any potential privacy risks. This would be updated each time ownership is changed so that there is an explicit awareness and inheritance of capabilities.

Participants discussed how to raise consumer awareness of privacy risks, especially as many people don't understand the full capabilities of and risks posed by the many IoT devices they use. As such, there needs to be a level of consumer understanding – based on what is being purchased, and a familiarity of the type of information that may be sent from devices. Others argued that it is a two-way street: the manufacturer should disclosure the device's purpose, the risk associated with it, and its intended use, while consumers need to be aware of the impact these devices can potentially have on their privacy.

Botnet Report Roadmap & Next Steps

Kevin Stine (NIST) and Evelyn Remaley (National Telecommunications and Information Administration [NTIA]) presented on a roadmap for combatting automated, distributed threats. Following the May 2018 release of the report, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Botnet Report), the Departments of Commerce

(NIST, NTIA) and Homeland Security (DHS) are developing a follow-on roadmap to coordinate actions to increase the resilience of the internet and communications ecosystem.

The roadmap, informed by stakeholder feedback, will provide a foundation for coordination and collaboration, increasing stakeholder confidence that resources invested in industry-led actions with federal dependencies will result in productive outcomes. Demonstrating US government commitment is a priority, and the roadmap will serve as a tool to identify stakeholders, key components and actions, and dependencies among the tasks. Workshops and other mechanisms will provide industry opportunities to share additional insights, and identify additional leaders within the community who might be able to assist with the recommendations and actions.

The roadmap is expected to be submitted to the White House in fall 2018. The Departments of Commerce and Homeland Security will work with industry and other stakeholders to track and regularly report on the progress made towards these activities and areas of effort.

NIST Next Steps

In September 2018, NIST intends to release a draft publication on considerations for managing IoT cybersecurity and privacy risks for public comment. Updates will be posted on the NIST Cybersecurity for IoT Program web site.

Feedback and Engagement

NIST is committed to maintaining an open dialogue. The community is encouraged to participate in this effort by providing feedback on the pre-read document, sharing insights, and emailing questions to iotsecurity@nist.gov. If you would like to watch the recordings of the plenary sessions during the workshop, you may do so here.