IoT Security and Privacy Risk Considerations

NIST Cybersecurity for IoT Program and Privacy Engineering Program

Purpose and Questions

This document provides background information on NIST's developing approach to Internet of Things (IoT) security and privacy and encourages discussion and feedback. The NIST Cybersecurity for IoT Program and the Privacy Engineering Program are seeking insights from stakeholders on these preliminary ideas for improving security and privacy risk management for IoT. NIST is considering developing guidance for federal agencies, though much of its content may be useful for other organizations. Listed below are the specific areas in which NIST seeks comments, but any constructive feedback will be considered.

NIST is looking forward to engaging with stakeholders in person and virtually. For those who cannot engage in-person, we encourage sending feedback to IoTsecurity@nist.gov.

Document Scope and Motivation

NIST proposes framing IoT as an ecosystem comprised of networked infrastructures[1] of connected objects[2] (devices, information, and people) that control or otherwise interact with the physical world through sensors and/or actuators.[3] These infrastructures enable the collection, processing, storage, and transportation of data, as well as taking action based on data, with or without human intervention.

Q1: Is a network connection to an external network required for devices to be considered IoT?

There are many definitions of IoT, but no single definition is widely used. NIST is scoping IoT for our guidance to cover the portions of IoT where organizations may be at greatest need of information on security and privacy risk management.

Our motivation for developing guidance is to enable organizations to characterize and manage the security and privacy risks associated with their IoT devices throughout the device lifecycles. This includes:

1. Emphasizing IoT is an evolution, not a revolution. It likely necessitates adjustments to existing practices, as well as new guidance for aspects not covered in existing practices.

Q2: We selected the term "devices" over terms such as "objects" and "things" as there does not seem to be consensus among technology, security, and privacy professionals on the preferred term. Which term would be best for future guidance?

---

[1] NIST is currently discussing whether IoT includes isolated network infrastructures—for example, a car with built-in IoT devices networked to each other but with no connection to the Internet or any other external network.

[2] The authors' use of "connected objects" instead of "networked objects" is deliberate. For example, sensors may be deployed in a hierarchical architecture, physically connected to each other through wires that are not part of a network. Because the IoT infrastructure encompassing the sensors is network-connected, the sensors may be at risk from network-based threats even though they are not networked.

[3] This scope intentionally omits the word "intelligence," which is often used to describe IoT. Many IoT devices do not have intelligence; for example, they may be programmed to initiate an action when an input value crosses a threshold, or they may simply collect data without performing analysis or making decisions.

2. Familiarizing organizations with common IoT capabilities and characteristics, thus enabling them to understand which assets are IoT devices.
3. Describing practical, high-level security and privacy risk management considerations for IoT devices throughout their lifecycles and specific to their environments.
4. Providing information on typical capabilities and characteristics - for example, IoT devices that may introduce security and privacy risks.

While we recognize there are many types of IoT risks to be managed – such as safety, reliability, resilience, and performance – we are solely focused on security and privacy risk. Important actions, such as conducting safety assessments and quantifying the potential impact to reliability of an IoT failure, while important considerations, are not in the scope of this effort. Our expected focus for the guidance is security and privacy risks for two types of IoT ecosystem components: integrated (e.g., off-the-shelf) IoT devices with built-in sensors and/or actuators, and composite IoT devices (two or more IoT elements working together to provide IoT functionality, such as a dynamic system with frequent sensor additions/removals).[4]

Q3: Our expected focus for the guidance is security and privacy risks for two types of IoT ecosystem components: integrated IoT devices with built-in sensors and/or actuators, and composite IoT devices.

Are these the areas where organizations need more guidance? Are there any others NIST should focus on?

Privacy and Security Risk Management

Privacy and security fields have the same objectives with respect to the security of personally identifiable information (PII) and limiting adverse consequences for individuals arising from unauthorized behavior in a system. However, individuals' privacy cannot be protected solely by securing PII. Thus, privacy risk management must also account for risks when the system's intentional or authorized processing of PII or individuals' interactions with the system may create problems or adverse consequences for these individuals.[5] Therefore, as used in this document, "privacy risk" means the potential for components of the IoT ecosystem to create adverse consequences for individuals regardless of whether the operations affecting individuals are authorized or unauthorized.

Managing IoT security and privacy risks involves a delicate balance among several factors, including the ability to identify and sufficiently characterize IoT devices; the accuracy and comprehensiveness of risk assessment and response actions; the usability of the tools and processes; the amount of time and human resources needed; and the limited effectiveness and unintended side effects of available risk mitigation methods.

We are currently considering which approaches may be effective for managing IoT security and privacy risks while balancing these important factors. Rather than creating a new risk management framework, the focus is on identifying how IoT risk differs from risk for other computing devices and providing information on what organizations should take into consideration in their risk management practices. It

---

[4] Other components of IoT device operations, such as cloud-based aggregation services, storage, and processing for IoT data, and network infrastructure components and other supporting parts of the IoT infrastructure, are only in scope for the NIST publication in terms of their interactions with integrated or composite IoT devices and their responsibilities for protecting IoT data. All non-IoT-related aspects of these components still require security and privacy risk management by the organization.

[5] More information on NIST's approach to privacy engineering and risk management is available in NIST Internal Report 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems.

is also critical to ensure the IoT security and privacy risk management approach is scalable to make the best use of available resources, as well as to recognize the differing levels of effort needed for varying IoT devices and deployment scenarios.

Identifying IoT Capabilities

To help organizations better identify IoT devices and document their characteristics, NIST is proposing several IoT capabilities. They encompass the entire IoT operating stack to provide a high-level structure for documenting what an IoT device is capable of doing. This structure could help organizations improve the consistency of privacy and security risk information gathering. The capabilities are:

Q4: Are there any gaps in this capabilities list?

- **Processing**, which provides the ability to transform data based on an executed algorithm. Data may be processed locally and/or remotely.
- **Storage**, which provides the ability to store and remove data, software and software settings, credentials, and other information over time on local and/or remote media.
- **Interfaces**, which provide the ability to transmit data unidirectionally or bidirectionally from one physical or logical location to another.
- **Sensing**, which provides the ability to sense an aspect of the physical or logical world. From NIST Special Publication 800-183, Network of 'Things,' a sensor measures physical properties such as "temperature, acceleration, weight, light, sound, location, presence, [and] identity," and provides data as its output.
- **Actuating**, which provides the ability to make a change in the physical world by receiving input, then physically controlling objects accordingly. Examples include heating coils, electronic door locks, servomotors, and robotic arms.
- **Software usage and management**, which provides the ability to acquire, verify the integrity of, configure, store, retrieve, execute, terminate, remove, and replace or update software. Examples of software include firmware, operating systems, functional applications (for example, aggregation software), and applications for managing the software itself.

Use Case Approach

NIST is considering whether to propose use cases as a tool to help organizations identify IoT-related considerations affecting security and privacy risk management. Developing a use case includes characterizing the IoT device – that is, understanding the device's operation and usage to the extent needed for the organization's risk management decision-making processes. Some characteristics are dependent on why the device is being used, how the device will be used, where the device will be deployed, etc.; these characteristics may significantly affect risk considerations.

Examples include:

- Inherent device characteristics (present regardless of how the device is used, where it is deployed, etc.);
- Business/mission value;
- Device usage (both intended use and unintended use);
- Device administration/management;
- Device location and environment;
- Data of interest (sensor data, credentials, software updates, etc.); and
- Security and privacy engineering objectives for the device and its data.

One device may have simple characteristics (has one sensor deployed in a secure, organization-controlled facility), while another device may have complex characteristics (has numerous sensors and actuators, transmits sensitive data to three systems, stores data locally and remotely, performs local processing, is deployed in a public area). By identifying these characteristics within the context of a use case, an organization can get a general sense of the likely effort needed for security and privacy risk management activities.

Q5: What use cases would best document interactions between IoT capabilities?

We may also need to document interactions between IoT capabilities. For example, two IoT components by themselves might each not seem particularly risky, but putting them together introduces new risks. We are particularly interested in gaining a better understanding of how organizations can identify noteworthy interactions for further analysis, what types of interactions should be documented, and how interactions should be characterized.

Risk Assessment and Response

After developing a use case, an organization should be prepared to assess risk and determine how to respond to it through risk acceptance, mitigation, transfer, or avoidance. We are considering how risk assessment and response processes may need to be adjusted to take into account IoT characteristics. For example, in the highest-risk situations, it may be most effective to identify and analyze risks involving each layer of the IoT stack using a data-centric system threat modeling approach, then determine how to respond to the risks for each layer.

Other approaches may be less resource-intensive and more suitable for a wide range of IoT devices. Options include:

- Identify risk scenarios for the IoT device that should be analyzed in order to assess risk. A risk scenario is a high-level description of a way security and privacy objectives could be negatively affected within an IoT ecosystem.
- Defining desired outcomes for IoT device security and privacy. An outcome provides a high-level statement that is similar to a risk scenario, but risk scenarios use negative language and outcomes use positive language. Outcomes would be consistent with the way the NIST Cybersecurity Framework (CSF) defines its subcategories, and current and target profiles could be defined for IoT device security and privacy outcomes.

Compared to sets of control requirements, approaches such as risk scenarios and outcomes allow for greater flexibility in how security and privacy are achieved, which makes them well suited to IoT's heterogeneous nature. Risk scenarios and outcomes are relatively easy for people to understand, making them further advantageous. High-level statements are helpful for communicating to all stakeholders, understanding the true potential impact of violations of IoT security and privacy objectives, and prioritizing organizational efforts. Lower-level statements developed by decomposing the high-level statements are needed for risk assessment and response, including mitigation control selection.

In terms of risk mitigation, NIST is interested about how controls may vary between IoT and non-IoT environments, and how organizations can compensate for those differences. For controls in scope, NIST guidance might indicate which types of controls are likely to be absent or impaired in IoT environments, and how organizations can add controls or reconfigure existing controls to compensate.

NIST also recognizes that mitigating controls may involve both pre-market and post-market options. Pre-market controls are implemented by the IoT device vendor; an example is controls that a device manufacturer implements in the device. Post-market controls are implemented by the customer organization. These controls include disabling all unneeded network interfaces; not transmitting unnecessary data; requiring mutual authentication of endpoints; and encrypting network communications end-to-end between sender and recipient. Each mitigation control should be labeled by the parties who would be responsible for implementing it (supply chain, manufacturer, administrator, end user, etc.).

Organizations will need to determine which control additions and changes are appropriate for their needs, such as estimating the effectiveness of each control alteration against each applicable risk, and estimating implications of control additions and changes (increased costs; reductions in functionality, usability, and performance). It is outside the scope of this effort to discuss these characteristics in detail, and they have been thoroughly covered in many existing publications.[6]

Q6: How could risk assessment and response processes be adjusted to take IoT characteristics into account?

Next Steps

The NIST Cybersecurity for IoT Program and Privacy Engineering Program will continue collaborating with stakeholders as this draft guidance is developed. The Program intends the guidance to have broad applicability for common security and privacy risks for IoT, and to introduce practical risk management considerations for IoT product selection, deployment, protection, and operation. As part of the drafting process, the Program will continue to engage with stakeholders for input on discussion drafts.

Updates on Program activities and collaboration opportunities are available on the NIST Cybersecurity for IoT Program website.

Discussion Questions

1. Is a network connection to an external network required for devices to be considered IoT?
2. NIST selected the term “devices” over terms such as “objects” and “things” as there does not seem to be consensus among technology, security, and privacy professionals on the preferred term. Which term would be best for future guidance?
3. Our expected focus for the guidance is security and privacy risks for two types of IoT ecosystem components: integrated IoT devices with built-in sensors and/or actuators, and composite IoT devices. Are these the areas where organizations need more guidance? Are there any others NIST should focus on?
4. Are there any gaps in the capabilities list? (See page 3)
5. What use cases would best document interactions between IoT capabilities?
6. How could risk assessment and response processes be adjusted to take IoT characteristics into account?

[6] For example, see NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations