Ideas for the Future of IoT Cybersecurity at NIST:

IoT Risk Identification Complexity

June 21, 2022

Introduction

NIST's work in cybersecurity for IoT has taken many paths. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228 explored how IoT could impact common cybersecurity goals for enterprise organizations. *Foundational Cybersecurity Activities for IoT Device Manufacturers*, NISTIR 8259 guided manufacturers of IoT devices in the area of developing their IoT devices with their customers' cybersecurity needs and goals in mind. *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, SP 800-213 provides federal agencies a process to adequately consider and mitigate the impacts of IoT devices on their information systems. Most recently, consumer IoT considerations[1] were developed as part of NIST's response to EO 14028 and included with recommendations for a consumer IoT product cybersecurity labeling program.

Through all this work, a consistent point of feedback has been the many challenges that characteristics of IoT create for risk identification. We have heard from IoT device manufacturers that IoT use and customer heterogeneity makes identifying and addressing all risks, for all possible customers essentially impossible. For customers, the complexities of IoT technologies and risks, as well as the black-boxed nature of IoT devices and products, leave customers of all kinds (e.g., home consumers, enterprise organizations) in the dark when they are confronted with the responsibility of securing these products on their networks. These challenges are not limited to one product type or sector.

This discussion paper will present some grounding for risk identification in IoT, based on NIST's prior work in cybersecurity for IoT (e.g., NISTIR 8259), and plot the path for forward-looking discussions on how to identify and address risks for IoT devices. Questions to consider when reading and to discuss:

1. What resources (e.g., frameworks, guidance) can manufacturers leverage when identifying risks of their IoT devices?
2. How can IoT device manufacturers approach risk identification and approach addressing those risks for multi-use/multi-customer IoT devices?
3. How can an IoT ecosystem (e.g., IoT products, their customers, manufacturers, other supporting parties) best manage identification of and addressing risks related to emergent use cases (i.e., those uses that were not expected by the IoT product manufacturers when initially designing the product)?

Next, some essential concepts from NISTIR 8259 for IoT risk identification and consideration are discussed, including a framework for thinking about known and emergent risk factors. Then, aspects of IoT technology heterogeneity are highlighted, followed by consideration of how IoT use case and customer context can further inform risk identification. Finally, the challenge of emergent customers and use cases is discussed.

[1] These considerations and the resulting technical and non-technical cybersecurity outcomes for consumer IoT products are now in draft as *Profile of the IoT Core Baseline for Consumer IoT Products*, Draft NISTIR 8425.

Risk Identification Considerations for IoT

IoT offers a wide array of use cases, each of which has cybersecurity needs and goals that need to be addressed by manufacturers through the IoT products they create. As NISTIR 8259 describes, a manufacturer can identify its expected customers and use cases for a product, then build the product to best address the needs and goals of those expected customers based on identified risks related to the IoT product. Creating an IoT product will bring together different technologies for the purpose; at least one transducer[2] and networking technology, which can have varying implications for risk, even at this most basic level. For example, many kinds of IoT device use a digital camera, but not always to capture and transmit images. Some cameras can be used to sense the environment (e.g., for temperature, motion), which may present different risks than a high-definition camera that streams video. The connectivity of IoT also means they will have processing, storage, and/or networking features, but some consumer IoT use cases will demand significantly more computing resources than others. IoT products may also contain multiple components in addition to the physical IoT devices, such as mobile apps or backends, which can bring additional considerations and further technological complexity. For an IoT product manufacturer, the technologies used to create a product, expected customers, and expected use cases are all known and can be used to inform how the IoT product should address cybersecurity needs and goals for customers. Figure 1 shows how technologies are utilized for use cases relevant to customers, with the entirety of that context being important for risk identification.

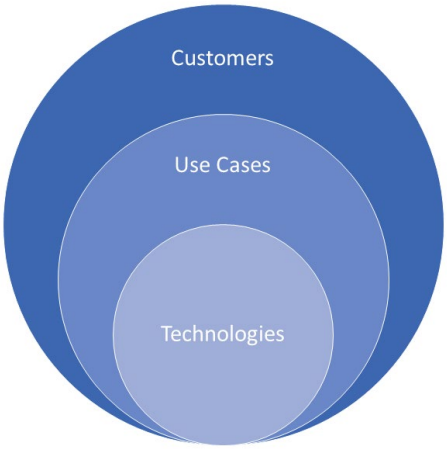

Figure 1 - IoT customers have use cases that technologies can fill

A key takeaway of Figure 1 is that technologies may be adopted for multiple use cases, which in turn may be relevant to multiple customers. When all use cases and customers can be anticipated and are expected, identifying all applicable risks and planning the best path to addressing those risks in the context of their customers' needs and goals will be challenging, but it is not common that all *possible* customers and use cases can be known. IoT products may be used by unexpected customers or for unexpected use cases even by expected customers in what can be called *emergent use cases*. For example, as consumers' homes accumulate more edge computing and network connectivity through further adoption of consumer IoT products, the home may become a nexus of consumers' digital lives. Healthcare, education and work are increasingly taking place remotely, allowing patients, caregivers, students, and teachers to interact and provide or access services using a foundational infrastructure in

[2] A transducer Is a sensor (e.g., thermometer, motion detector) or actuator (e.g., speaker, door lock).

individuals' homes (e.g., internet connectivity, PCs and smartphones). Consumer IoT products may expand this infrastructure, allowing for use of these products in telehealth and education systems, and thus increasing interactions and integration between enterprise/industrial systems and a variety of IoT products. Table 1 identifies key factors of risk identification for IoT products and discusses possible implications they may have on risk identification, and further, addressing of customer's needs and goals.

Table 1 - Known and emergent factors of risk identification and their possible implications.

	Risk Identification Factor	Possible Implications
Known Pre-Market	**IoT Product Technology** – IoT products are created using multiple technologies that bridge the physical and digital worlds	● Nature of the technologies used to build an IoT product helps inform risk identification and aspects of cybersecurity needs and goals (e.g., kinds of data collected/used by the product, other risk domains impacted by the technologies)
	IoT Product Expected Customers and Use Cases – IoT products will be developed to fill a specific use case for certain customers	● The customers of a product and how the technologies are used by them can help identify interactions with physical and digital entities and related risk considerations ● Understanding the expected customers and their needs and goals for a use case in response to the risks identified related to the IoT product informs manufacturers of what support for the customer would be adequate for those needs and goals
Emergent Post-Market	**Unexpected Use Cases by Expected Customers** – Expected customers may use the IoT product in ways and environments the manufacture did not consider or intend	● May introduce unexpected interactions with unplanned physical or digital entities with divergent or unique risks ● IoT product may not adequately support the cybersecurity needs and goals for unexpected use cases which may carry altered risks relative to expected use cases
	Unexpected Customers/Third Parties – Other kinds of customers that may be very different in needs and goals may use the IoT product	● Unexpected customers may connect the product with unexpected technologies that can introduce entirely new risks ● Unexpected customers' needs and goals (e.g., risk appetite, approach to risk mitigations) may vary significantly from expected customers'

As Table 1 summarizes, though these factors may have varying cybersecurity implications, they generally represent a set of unknown challenges that are difficult for IoT product manufacturers to adequately address. For some unexpected customers or use cases, responsibility for augmenting the cybersecurity capabilities of an IoT product to meet the needs and goals for the situation would be the responsibility of the customer. For example, in the case of telehealth applications that use a customer's home system to deliver services, the telehealth provider may be responsible for cybersecurity of the overall system, including connections with home IoT products. In other cases, such as a home consumer using the same technology for a small business poses more complicated questions about how the customer's needs and goals can be best addressed. Over time, as unexpected uses become known and more common, manufacturers can help customers by incorporating them into the needs and goals they consider as part of the product development process (e.g., by incorporating the needs and goals into those they support or alerting customers that the use case is not directly supported).

IoT Technology Heterogeneity

Most IoT products are inherently heterogeneous in their composition: combining networking capabilities with transduction capabilities. An IoT device will combine networking and computing technologies with sensing and actuating modules. These devices may be further supported by other kinds of technology such as a real-time control network, a controller console and/or app, often a cloud server or private server, wireless and/or wired networks, and a wide variety of other components. For example, an IoT device may collect and package data to be transmitted via any number of communications protocols to a local (e.g., sensor hub) or remote (e.g., cloud or dedicated back end) data aggregator, where the data can be used to generate new data, possibly even commands that are sent back to the IoT device.

When manufacturers recognize the heterogeneity factors within their IoT products they are better able to identify the risks throughout all the IoT product components. IoT technology heterogeneity within a device/product can bring together many disparate risks (e.g., network-based attack risks when a product is internet connected, ransomware risks due to operational necessity) and even create a variety of unique risks for the specific combination of technologies. IoT products vary greatly. On one end of the spectrum are IoT devices with various types of significant resource constraints (e.g., processing power, energy, storage, transmission speed/quality), and on the other are highly complex and dynamic IoT products comprised of multiple transduction modalities and various types of sub-systems. These differences can change how common cybersecurity needs and goals are supported by the IoT product and manufacturer, but as the next section highlights, are only part of the set of information a manufacturer will use to identify customers' needs and goals based on risks and how to support them.

Heterogeneity in Customer and Use Case

For IoT products, there is a wide range of customers and use cases for which risks will vary based upon context of use. Though cybersecurity risks can be similar for IoT products with comparable computing, connectivity, and features, additional considerations about *how* the product will be used by customers (i.e., its use case) can change those risks and/or the appropriate support expected by the customer from the IoT product and manufacturer. For example, a small speaker that is intended to be used as a fire alarm will likely have increased integrity and availability expectations relative to a similarly architected speaker intended to be used as a wake-up alarm. *Who* is to use the IoT product must also be considered to determine the pertinent risks and especially appropriate support to help customers address those risks. Industrial IoT product customers may need different cybersecurity capabilities than home IoT product customers, even for a similar use case. An automated robot that operates in a home (e.g., smart vacuum) will be used differently and have different expectations placed upon it compared to a robot used in a public setting (e.g., aisle monitoring robot in a supermarket).

Another complicating factor for IoT risk identification is the interplay of cybersecurity risks with other forms of risk (e.g., safety, privacy) that IoT products may face contextually based on their technologies, customers, and use cases. Sometimes cybersecurity risks/mitigations will harmonize with the additional risk considerations. For example, confidentiality issues regarding public access to images from consumer security cameras intended to be used within the home would be closely related to privacy and perhaps physical safety risks associated with such a design. It is also possible that cybersecurity risks and other risks may conflict. For example, on a factory floor, high levels of data availability and sharing could pose a significant risk to data confidentiality, but may be critical to safety.

The abundance of IoT use cases and the diversity of IoT product implementations makes risk identification for IoT a challenging task for many ecosystems. Further, customers may have divergent cybersecurity expectations even for similar use cases, further complicating the task of a manufacturer identifying and addressing risk based on their customers' needs and goals since they may not be uniform for all customers.

Emergent Use Cases

NISTIR 8259 discusses how a manufacturer can plan for expected customers and use cases of their IoT devices during the pre-market phase of development. In the post-market phase, as time goes on, additional uses for the IoT device may appear from expected or even unexpected customers. Figure 2 shows how an IoT device and any other components that may create an IoT product can have a set of expected use cases and customers that diverge from an emergent customer and their use cases.

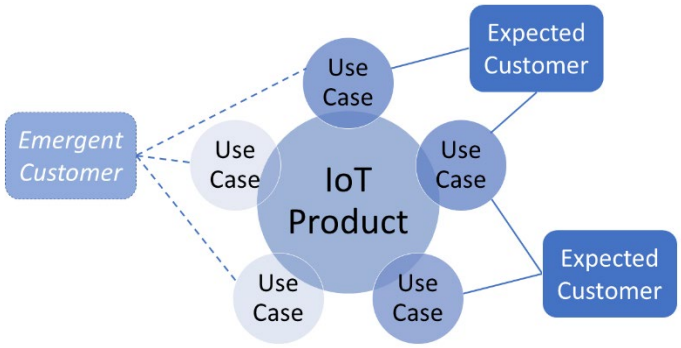

Figure 2 - Emergent customers can have the same or different/new use cases compared to expected customers

This phenomenon of emergent customers and use cases poses a challenge for IoT because of the dynamic nature of IoT adoption and use, and sometimes conflicting demands of disparate customers and use cases. These sum to make planning for emergent use cases of IoT product more challenging than for some other technological domains. An emergent customer or use case for an IoT product may bring risks so different from the intended customer/use case that the IoT product and manufacturer cannot ever support the emergent case. Technology considerations may further limit support for emergent use cases, especially for constrained devices or IoT products developed with technologies only fit for some customers within a use case (e.g., kitchen scales vs. postal scales vs. rated scientific/industrial scales).

At the same time, emergent use cases can be beneficial for customers, society, and even the manufacturers to foster and support. Where possible, off-the-shelf IoT products being usable for broad sets of customers and use cases can help reduce costs, increase efficiencies, foster adoption, and increase the cybersecurity of IoT overall. For example, an enterprise customer can likely save costs by using consumer-grade IoT that is suitable for their purposes, avoiding more costly IoT products that may be unnecessarily overfitted for enterprises. Or, services such as telehealth can be improved by tapping into common or easily available consumer IoT health products. Identification of emergent use cases, their associated risks, and adequate support that can be provided by the IoT product and manufacturer is a significant challenge for the IoT community.

Conclusion

These ideas are developing and are meant to spur conversation, consideration, and discussion among stakeholders before and at our upcoming workshop planned for June 22nd, 2022. Some have been addressed to some degree in our prior work, but there has been repeated request for NIST to approach the complexities of IoT risk identification as a topic on its own. NIST welcomes thoughts and discussion on the challenges highlighted in this essay and how NIST can support the community.