"Security and Privacy Considerations for IoT" Pre-Read Essay

NIST Cybersecurity for IoT Program

Introduction

On October 19th, 2017, the National Institute of Standards and Technology (NIST) is hosting the IoT Cybersecurity Colloquium to convene stakeholders from across government, industry, international bodies, and academia. Our goal is to better understand the concerns and threats associated with the rapidly broadening landscape of connected devices, known as the Internet of Things (IoT).

In advance of this event, the **NIST Cybersecurity for IoT Program** asks participants to come prepared to share their perspectives on a variety of questions, presented at the end of this document. In general, the Program is particularly concerned with understanding the community's drivers and concerns around IoT adoption and how NIST might best help address those concerns. Questions, insights, and responses to the questions at the end of this document can be submitted to iotsecurity@nist.gov.

Additionally, as this essay acknowledges, the expanding IoT landscape is subject to an equally expanding list of threats, attacks, and corresponding outcomes. To address this, NIST is seeking to understand whether grouping devices based on characteristics or capabilities would be useful for identifying specific threat profiles and determining appropriate mitigation strategies.

Background

The diverse use and rapid proliferation of connected devices creates enormous value for industry, consumers, and broader society. Gartner predicts that there will be 20.4 billion connected devices in use by 2020. [1] It sounds like a longshot, but take into consideration that number was 6.5 billion in 2016[2], up from 3.8 billion in 2014 and 4.9 billion in 2015.[3] Given the staggering number of connected devices already in use, it's reasonable that in four years, most of the "things" we interact with will be part of the IoT ecosystem.

Connected devices sense, collect, process, and transmit a wide array of data. This may include anything from consumers' personally identifiable information and proprietary company data, to infrastructure data used to make critical real-time decisions or effect a change in the physical world. These devices are seemingly everywhere – from medical devices to cars to manufacturing floors – and carry a promise of enhanced business efficiencies and increased consumer satisfaction. However, as the variety of uses grows, so too do the threats that could undermine individual devices and the broad Internet of Things (IoT) ecosystem.

NIST's 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

[1] http://www.gartner.com/newsroom/id/3598917
[2] Ibid.
[3] http://www.gartner.com/newsroom/id/3165317

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.

The need for IoT cybersecurity is increasingly clear. In September 2016, Mirai malware was used to create large botnets, which included IoT devices, that executed a distributed denial-of-service (DDoS) attack on the security blog Krebs on Security. This was one of the largest DDoS attacks on record – according to the malware's author, the attack used more than 380,000 devices.[4] The malware's source code leaked later that month, leading to others using Mirai to create other large botnets. In October 2016, Mirai was employed to target Dyn, an internet infrastructure company, ultimately taking down many major websites for a large part of the day.[5]

IoT devices may also introduce privacy risks that extend beyond traditional data security. For example, the ubiquity of these devices poses challenges for managing information collection about people, and for helping people understand how their information is being used.

Understanding IoT

There are a vast number of IoT capabilities and solutions in the marketplace, and the federal government is increasingly adopting them: in 2015, the federal government spent $8.8 billion on IoT technology.[6] The following examples, while far from comprehensive, help to illustrate the reach of the IoT ecosystem and the associated security and privacy challenges.

- Connected vehicles "access, consume, and create information and share it with drivers, passengers, public infrastructure, and machines including other cars."[7] This enables vehicles, roads, and smartphones to share vital information. The ability for these components to communicate with one another could drastically reduce the amount of accident-related fatalities and injuries. Previously, the focus was on helping people survive crashes. Now, the U.S. Department of Transportation is looking to leverage connected vehicles to prevent these crashes from occurring: cars could communicate so each vehicle is aware of the location of the others and drivers would be notified of hazardous situations.[8]
- There is no shortage of IoT use in the world of healthcare – devices range from wearable fitness trackers to wireless infusion pumps, deployed everywhere from the user's home to a government-run hospital facility. IoT devices gather, transmit, and analyze data, including personal health information (PHI). This may introduce threats not present with traditional devices. For example, the wireless infusion pump's ecosystem – the pump, the network, and the data stored in and on a pump – may face a variety of potential threats including unauthorized access to PHI, changes to prescribed drug doses, and interference with a pump's function.[9]

---

[4] https://www.us-cert.gov/ncas/alerts/TA16-288A
[5] https://krebsonsecurity.com/tag/mirai-botnet/
[6] https://www.informationweek.com/iot/federal-iot-spending-hit-nearly-$9-billion-in-2015/d/d-id/1326495?
[7] https://www.technologyreview.com/s/426523/your-connected-vehicle-is-arriving/
[8] https://www.its.dot.gov/cv_basics/cv_basics_what.htm
[9] https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8a-draft.pdf

- Smart manufacturing includes software and sensors that allow for precise predictions of maintenance needs, material demand, and other factors, based on data captured through all points of production. However, the volume of unstructured data generated that could be consumed in big-data projects creates new kinds of considerations for security. The variety and size of this big data is too new for security personnel to understand what constitutes normal behavior and identify irregularities. Security professionals need to comprehend the analytics and automation being applied to determine how best to protect a big-data enterprise, because there is currently no practical way to fully maintain situational awareness of the data at the accelerated rates of acquisition and change.

Fundamental Motives for Using IoT

It's easy to understand the appeal of IoT devices; when successfully deployed they can improve efficiency and accuracy in a wide variety of tasks. Fundamental motivations for using IoT devices might be generalized into three categories:

- The ability to provide internet connectivity for devices that did not previously have connectivity, which enables remote control of these devices. This includes monitoring, configuration, troubleshooting, management, and other related functions.
- The ability to analyze data regarding the physical world. These data can inform decision making, alter the physical environment, and predict future events.
- The "smartness" of IoT. This refers to adding computing functionality that similar devices previously lacked, supporting new functionality, services delivery mechanisms, and communications channels.

Addressing IoT Risks

NIST regards IoT as evolutionary, not revolutionary. That is, it emerged through combing existing technologies and capabilities. As such, and given the diverse uses of IoT technologies and environments, NIST expects there cannot be a "one size fits all" approach to identifying and mitigating security and privacy risks. To best address this varied threat landscape, NIST believes it could be beneficial to establish a characteristic-based way to discuss the various types of IoT ecosystem components.

Assuming there can be no "one size fits all" approach for IoT security and privacy, NIST anticipates that different types of systems may have different risk considerations. While market verticals alone do not suffice to determine what risks a system introduces, an understanding of how the system behaves may. Particular IoT capabilities, behaviors, and architectures will likely have their own sets of risk to consider.

In addition to potentially exacerbating existing risks, IoT, by its very nature, introduces new threat vectors and risk considerations. When assessing their particular risk profile, an organization must consider the nature of a specific IoT device and identify any associated threats.

As the Program has learned through stakeholder outreach, the list of threats is extensive. It includes – but is far from limited to – opportunities for malicious actors to highjack communication channels, change sensor data, access sensitive information, disrupt vital services, and alter signals and data for nefarious purposes. Outcomes range from the collection of bad data to actual, physical harm.

About the IoT Cybersecurity Colloquium

Stakeholders have expressed interest in NIST producing guidelines to help federal agencies understand and manage cybersecurity and privacy risks associated with the use of IoT.

The IoT Cybersecurity Colloquium[10], hosted by NIST at its Gaithersburg campus on October 19, 2017, will focus on challenges organizations face in managing the security and privacy risks associated with the Internet of Things. Speakers from industry, academia, and government will explore the current threat landscape, challenges and considerations specific to the IoT ecosystem, as well as introduce practical risk management considerations for IoT deployment, protection, and operation over the course of the device lifecycle.

Questions to Address

NIST seeks to hear from stakeholders about IoT security and privacy concerns, and understand practical cybersecurity and privacy risk management considerations for IoT. To inform these topics, and possible next steps, NIST seeks stakeholder input on the following. Please send any feedback to iotsecurity@nist.gov.

1. What are the primary motivations for IoT adoption in your organization?
2. Which IoT characteristics pose the greatest security and privacy risks to your organization?
3. What aspect of the IoT ecosystem is your organization most concerned about? How could NIST help address these concerns?
4. Is there sufficient information on how to assess IoT risk and implement controls to mitigate these risks?
5. How have security and privacy risks increased with the deployment of connected devices?
    a. Which aspects of IoT deployment have created the most risk for your organization?
    b. What resources has your organization leveraged to address risk and apply security controls?
6. Is there sufficient guidance to support the acquisition processes geared towards secure and privacy-protective devices?
7. Would characteristic- or capabilities-based groupings of devices be useful for identifying your organization's threat profile and determining mitigation strategies?
8. What guidance would be most valuable for securing IoT?
    a. E.g. configuration; network connection; general control selection, design, and implementation; or patching and maintenance
9. What guidance would be most valuable for privacy protections for IoT?
    a. E.g. sensor information collection; people-device interaction; general control selection, design, and implementation

[10] https://www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium