Fall 2022

Cyber-Security and IoT Devices

Timothy Okrey

CYBER-SECURITY AND IoT DEVICES

By

Okrey, Timothy
AS, Moraine Valley Community College, 1984
BA, Governors State University, 1996
MS, Governors State University, 2020

THESIS

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science,

With a Major in Information Technology

Governors State University
University Park, IL 60484

2022

ABSTRACT

With the rapid rise of IoT devices, what sort of security concerns exist and what is being done about it. This paper will attempt to ask and answer these questions. The topic is clearly broad but every effort is made to narrow the work down to elements that are most common amongst IoT devices rather than exploring a particular product or product line.
.

Table of Contents

1. Introduction

The Internet of Things or IoT for short is a generic name that applies to any device connected to the internet. There are serious security and design concerns with respect to these devices. Manufacturers are trying to compete for market share and as such, the rate of innovation is quite staggering. These points were the target of my research with the intent of trying to determine the effect that this progress is having on the safety/security of said devices. What is the overall attitude of manufacturers with regards to the security of the devices they produce? I suggest that the position of manufacturers is to declare older unsecure models as no longer supported rather than make patches available.

There was an IEEE Symposium back in 2015 that demonstrates how long this question has been asked and offers some of the issues that arise in the security of IoT. Please refer to Basu, S. S., Tripathy, S., & Chowdhury, A. R. (2015). Design challenges and security issues in the Internet of Things. *2015 IEEE Region 10 Symposium*. "Connecting constrained devices directly to the Internet introduces a number of security loopholes primarily because these devices do not have the computational power to execute standard encryption techniques." It was my intent to ascertain whether or not progress is being made in closing the security loopholes. The approach was to try and identify the loopholes that are common to IoT devices. Then look at what proposed solutions are put forward to remediate the issues identified.

As the research began it was discovered that the National Institute of Standards and Technology or NIST had published quite a few documents to help drive standards for manufacturers to follow. There are several different publications and far too many to review for this paper. As the documents were being reviewed it became more apparent that the guidance from NIST was actually quite good and did lay a foundation for manufacturers to follow. Nomenclature and naming conventions were being introduced to permit a common language amongst them.

With this in mind, an effort was made to understand the guidance given by the NIST specifically with regards to Cybersecurity. The following section is the result of reviewing

the documentation and rather than just copying the content of the publications directly, some summarizing of the material was done.

2. NIST Standards

Diving into the standards defined by NIST we find several different components to try and create a comprehensive outline or guidance for manufacturers to follow.

2.1 Iot Device Cybersecurity Capability Core Baseline

The first one to review is called IoT Device Cybersecurity Capability Core Baseline which is found in NIST.IR.8259A. Much of the following content is found in this publication. The document has multiple tables within it but each table has four columns. The columns are used to help clarify each capability. The column Common Elements enumerate aspects of the capability. The column Rationale further ties the capabilities together.

This baseline, as it is called, is intended to help identify ways to assist manufacturers of IoT devices to manage and mitigate risk. There are six capabilities in this baseline:

I. Device Identification
II. Device Configuration
III. Data Protection
IV. Logical Access to Interfaces
V. Software Update
VI. Cybersecurity State Awareness.

Each of these capabilities are thought through so as to provide common language for manufacturers to use if they so choose. Let's take a deeper look at each of these capabilities.

2.1.1 Device Identification

The IoT device can be uniquely identified logically and physically. This is similar to the function of the MAC address on Ethernet devices. The documentation states that reasons for having a unique ID range from asset management to vulnerability management. Thus allowing for automated methods of controlling/managing the device.

2.1.2 Device Configuration

The IoT device can be configured and the configuration can be changed as needed. Add security to the device and this permits controlling who gets to make changes to it. This then permits for vulnerability management to be taken care of. The absence of the ability to configure the device limits the functionality of it.

2.1.3 Data Protection

The IoT device can use cryptography to secure the data on the device. This can be further extended to include data at rest as well in transit. Features of data protection are

further delineated as access management and incident detection.

2.1.4 Logical Access to Interfaces

The Iot Device can restrict access to any interfaces that it has as well as any services or protocols utilized by the device. Access can be partially or completely denied based upon the state of the device.

2.1.5 Software Update

The IoT device is able to be updated and only by authorized personnel or methods. This capability allows for not only updates but also rollbacks in the event that an update had issues.

2.1.6 Cybersecurity State Awareness

The IoT device is able to both know it's Cybersecurity state but is also able to report it. This permits the device to make other entities aware of it's state.

2.2 Foundational Cybersecurity Activities for IoT Device Manufacturers

This publication is found in NIST.IR.8259 and was published in May 2020. The contents of the document speak directly to the questions raised in the introduction, namely, what the manufacturer's attitude towards their devices should be. Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). "The main audience for this publication is IoT device manufacturers. This publication may also help IoT device customers that use IoT devices and want to better understand what device cybersecurity capabilities they may offer and what cybersecurity information their manufacturers may provide."

Further down in this publication as part of the Executive Summary we find Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). "The purpose of this publication is to give manufacturers recommendations for improving how *securable* the IoT devices they make are. This means the IoT devices offer *device cybersecurity capabilities*—cybersecurity features or functions the devices provide through their own technical means (i.e., device hardware and software)—that customers, both organizations and individuals, need to secure the devices when used within their systems and environments. IoT device manufacturers will also often need to perform actions or provide services that their customers expect and/or need to plan for and maintain the cybersecurity of the device within their systems and environments. From this publication, IoT device manufacturers will learn how they can help"

The document breaks up the manufacturer's guidance into a pre-market and post-market view. The first four sections are categorized as pre-market and the final two are

considered post-market. The following are excerpts from the publication.

2.2.1 Activity 1: Identify Expected Customers and Define Expected Use Cases

In this section the manufacturers are being encouraged to think about their audience as they design the IoT device. Questions to consider are listed as and taken directly from the publication:

I. Which types of people are expected customers for this device?
II. Which types of organizations are expected for this device?
III. How will the device be used?
IV. Where geographically will the device be used?
V. What physical environments will the device be used in?
VI. How long is the device expected to be used for?
VII. What dependencies on other systems will the device likely have?
VIII. How might attackers misuse and compromise the device?
IX. What other aspects of device use might be relevant to the device's cybersecurity risks?

2.2.2 Activity 2: Research Customer Cybersecurity Needs and Goals

This portion of the publication covers trying to ascertain the customer's needs. As explained Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). "Cybersecurity needs and goals will be primarily, but not entirely, driven by the cybersecurity risks they face. Manufacturers cannot completely understand all of their customers' risks because every customer, system, and IoT device faces unique risks based on many factors." As before, the following is taken directly from the publication:

I. How will the IoT device interact with the physical world?
II. How will the IoT device need to be accessed, managed and monitored by authorized people, processed, and other devices?
III. What are the known cybersecurity requirements for the IoT device?
IV. How might the IoT device's use of device cybersecurity capabilities be interfered with by the device's operational or environmental characteristics?
V. What will the nature of the IoT device's data be?

VI. What is the degree of trust in the IoT device that customers may need?

VII. What complexities will be introduced by the IoT device interacting with other devices, systems, and environments?

2.2.3 Activity 3: Determine How to Address Customer Needs and Goals

The guidance contained within this section focuses on how to address the needs and goals previously identified. This involves mitigating cybersecurity risks. From the publication Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). "For each cybersecurity need or goal, the manufacturer can answer this question: **which one or more of the following is a suitable means (or combination of means) to achieve the need or goal?**" As before, the following is taken directly from the publication:

I. The IoT device can provide the technical means through its device cybersecurity capabilities.

II. Another device related to the IoT device can provide the technical means on behalf of the IoT device.

III. Other systems and services that may or may not be acting on behalf of the manufacturer can provide the technical means.

IV. In addition to and support of technical means, non-technical means can also be provided by manufacturers or other organizations and services acting on behalf of the manufacturer.

V. The customer can select and implement other technical and non-technical means for mitigating cybersecurity risks.

The second portion of the guidance discusses the robustness of the solution. From the publication Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). "In addition to identifying suitable means for addressing each cybersecurity need and goal, manufacturers can also answer this question related to the technical means provided through their IoT device: **how robustly must each technical means be implemented in order to achieve the cybersecurity need or goal?**" Again we are taking the following directly from the publication:

I. Whether it needs to be implemented in hardware and/or software.

II. Which data needs to be protected, what types of protection each instance of data needs.

III. How strongly an entity's identity needs to be authenticated before

granting access if the entity is a human or system/device.

IV. Whether data received by or inputted into the device needs to be validated.

V. How readily software updates can be reverted if a problem occurs.

It is at this point in the documentation that they refer to NISTIR 8259A, the other publication that has already been reviewed in this paper.

2.2.4 Activity 4: Plan for Adequate Support of Customer Needs and Goals

Contained within this section are statements encouraging the manufacturers to adequately consider the correct level of resources required for their device to function properly. The following is directly from the publication:

I. Considering expected terms of support and lifespan, what potential future use needs to be taken into account?

II. Should an established IoT platform be used instead of acquiring and integrating individual hardware and software components?

III. Should any of the device cybersecurity capabilities be hardware-based?

IV. Does the hardware or software include unneeded device capabilities with cybersecurity implications? If so, can they be disabled to prevent misuse and exploitation?

There is a second set of questions at this point in the publication. These questions are around secure development practices. As before the following is taken directly from the publication:

I. How is IoT device code protected from unauthorized access and tampering?

II. How can customers verify hardware or software integrity for the IoT device?

III. What verification is done to confirm that the security of third-party software used within the IoT device meets the customers' needs?

IV. What measures are taken to minimize the vulnerabilities in released IoT device software?

V. What measures are taken to accept reports of possible IoT device software vulnerabilities and respond to them?

VI. What processes are in place to assess and prioritize the remediation of all vulnerabilities in IoT device software?

2.2.5 Activity 5: Define Approaches for Communicating to Customers

Activity 5 is focused on the manufacturer's responsibility with respect to communicating with customers. The goal of the guidance here is from Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). "Manufacturers of IoT devices will at some point market and sell their product, which will put it in the hands of customers and initiate the manufacturing post-market phase. Even in this phase, while customers are evaluating potential product acquisitions, and after IoT devices are sold to customers, manufacturers continue to have a role in supporting the customers' cybersecurity needs and goals and the IoT devices."

The following is taken directly from the publication:

I. What terminology will the customer understand?
II. How much information will the customer need?
III. How/where will the information be provided?
IV. How can the integrity of the information be verified?
V. Will customers have to communicate with you as the manufacturer?

2.2.6 Activity 6: Decide What to Communicate to Customers and How to Communicate It

Activity 6 is quite detailed and has many subsections all surrounding the idea of customer communication. Each subsection has multiple questions and as before they will be taken directly from the publication:

2.2.6.1 Cybersecurity Risk-Related Assumptions

The point made in this section is that the manufacturer's view of expectations may differ from the customer.

I. Who were the expected customers?
II. How was the device intended to be used?
III. What types of environment would the device be used in?
IV. How would responsibilities be shared among the manufacturer, the customer, and others?

2.2.6.2 Support and Lifespan Expectations

As is implied by the name of the section, it discusses expectation of support and lifespan. The following questions are taken directly from the publication:

I. How long do you intend to support the device?
II. When do you intend for device end-of-life to occur? What will be the process for end-of-life?
III. What functionality, if any, will the device have after support ends and at end-of-life?
IV. How can customers report suspected problems with cybersecurity implications, such as software vulnerabilities, to the manufacturer? Will reports be accepted after support ends? Will reports be accepted after end-of-life?
V. How can customers maintain securability even after official support for the device has ended? Will essential files or data be made available in a public forum to allow others, even the customers themselves, to continue to support the IoT device?

2.2.6.3 Device Composition and Capabilities

Our publication now attempts to provide guidance about how to communicate device specific information to the customers. The following question are taken directly from the publication:

I. What information do customers need on general cybersecurity-related aspects of the device, including device installation, configuration, usage, management, maintenance, and disposal?
II. What is the potential effect on the device if the cybersecurity configuration is made more restrictive than the default?
III. What inventory-related information do customers need related to the device's internal software, such as versions, patch status, and known vulnerabilities? Do customers need to be able to access the current inventory on demand?
IV. What information do customers need about the sources of the device's software, hardware, and services?
V. What information do customers need on the device's operational characteristics so they can adequately secure the device? How should this information be made available?

VI. What functions can the device perform?
VII. What data type can the device collect? What are the identities of all parties that can access that data?
VIII. What are the identities of all parties who have access to or any degree of control over the device?

2.2.6.4 Software Updates

Guidance is given about communicating a manufacturer's intent regarding updates and policies accordingly with customers. The following questions are taken directly from the publication:

I. Will updates be made available? If so, when will they be released?
II. Under what circumstances will updates be issued?
III. How will updates be made available or delivered? Will there be notifications when updates are available or applied?
IV. Which entity is responsible for performing updates? Or can the customer designate which entity will be responsible?
V. How can customers verify and authenticate updates?
VI. What information should be communicated with each individual update?

2.2.6.5 Device Retirement Options

Further guidance to manufacturers about how to communicate retirement options to customers. The following questions are taken directly from the publication:

I. Will customers want to transfer ownership of their devices to another party? If so, what do customers need to do so their user and configuration data on the device and associated systems are not accessible by the party that assumes ownership?
II. Will customers want to render their devices inoperable? If so, how can customers do that?

2.2.6.6 Technical and Non-Technical Means

The publication is attempting to delineate the difference between device cybersecurity capabilities and those actions required by a customer. The following questions are taken directly from the publication:

I. Which technical means can be provided?
    a. By the device itself

b. By a related device?
c. By a manufacturer service or system?

II. Which non-technical means can be provided by the manufacturer or other organizations and services acting on behalf of the manufacturer?

III. Which technical or non-technical means should the customer provide themselves or consider providing themselves?

IV. How is each of the technical and non-technical means expected to affect cybersecurity risks?

3. Literature Review

The previous section was all about digesting just two publications specifically creating guidance for IoT manfucturers. This guidance is voluntary and was published in May 2020. Most of the articles that were located predated these NIST publications. With this in mind reviewing the documented concerns in the various articles demonstrate the need for the aforementioned documents. The first article was published in November 2016 and refers to an actual event. See Lemos, R. (2016). [On Nov 16 security experts plan to testify in front of two subcommittees in the U.S. House of Representatives, warning Congress that a lack of focus on security has made the Internet of Things a playground for hackers.

The hearing follows the October attacks against Internet-infrastructure provider Dyn, which struggled for more than 11 hours to mitigate a flood of data that caused its domain services to become unreachable and resulted in intermittent service outages for its clients, including Twitter, Netflix, Etsy, Paypal and Spotify.

"These new attacks are alarming for their scope, impact and the ease with which attackers employed them," Dale Drew, chief security officer of Internet provider Level 3 Communications, stated in prepared comments to be delivered at the hearing. "Also worrisome is that these attackers relied on just a fraction of the total available compromised IoT nodes in order to attack their victims, demonstrating the potential for significantly greater havoc from these new threats."]

The NIST Publication NIST.SP.800-183 outlines elements of the items we refer to as Things. This publication was authored by Jeffrey Vaos in 2016. He later co-wrote a summary document that was published in the May/June issue of IEEE's website

www.computer.org/itpro. This summary document led to a fascinating comment found in Voas, J. M. (2016). [Since data is the "blood" of a NoT, communication channels are the "veins" and "arteries", as data moves to and from intermediate events at different snapshots in time.] This statement gets to the heart of the concern and clearly articulates the potential value in the data being processed via IoT devices.

Searching through the various publications and the NIST guidance there are several documents written specifically to address the concerns outlined in the introduction. The detailed breakdown of this document was in section 2 of this paper, but now refer to NIST.IR.8259A to discover the IoT Device Cybersecurity Capability Core Baseline. The intent of this document can be found in Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020b). "The purpose of this publication is to give manufacturers recommendations for improving how *securable* the IoT devices they make are. This means the IoT devices offer *device cybersecurity capabilities*—cybersecurity features or functions the devices provide through their own technical means (i.e., device hardware and software)—that customers, both organizations and individuals, need to secure the devices when used within their systems and environments. IoT device manufacturers will also often need to perform actions or provide services that their customers expect and/or need to plan for and maintain the cybersecurity of the device within their systems and environments. From this publication, IoT device manufacturers will learn how they can help"

Another article published in March 2019 summarizes the security concerns surrounding IoT Devices as follows, please refer to Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., … Elovici, Y. (2019). "IoT devices may pose major security and privacy risks, because of their range of functionality and the variety of processes involved in their operation, including data collection, processing, storage, and transfer—by, from, and to these smart devices [22], [23]. Furthermore, these smart devices are integrated in enterprise networks, deployed on public spaces, and worn on the body and can be operated continuously in order to gather information from their surroundings; hence, they are highly visible and accessible—especially to attackers. In the following subsections, we discuss security and privacy aspects related to device architecture, network connectivity, and the type of data collected by IoT devices. In addition, we present

countermeasures to reduce and mitigate the problems discussed."

Looking into other types of IoT devices an article published in 2018 was found outlining best practices for implementing a smart home. There is an interesting quote from this rather exhaustive document. Please refer to Batalla, J. M., Vasilakos, A., & Gajewski, M. (2018). "General security requirements for Smart Home infrastructure cover six well-known goals: confidentiality/privacy, integrity, authenticity, non-repudiation, availability, and authorization. However, unlike Internet-connected terminals, most Smart Home equipment neither have a uniform execution environment nor enough computational power. Therefore, it is difficult to implement a complex security strategy. Since the Smart Home environment partially inherits its components from IoT systems, some security-related categories describing IoT platforms may also be applied to Smart Homes, specifically as regards the WSNs." The point here that caught my attention was the part where the authors refer to non-uniform execution and not enough computational power."

Further studying found an attempt to address intrusion detection among IoT devices. This paper discusses the topic at great length but the abstract caught my attention because it speaks about two specific events, one we already mentioned. Please refer to Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). "Pervasive growth of Internet of Things (IoT) is visible across the globe. The 2016 Dyn cyberattack exposed the critical fault-lines among smart networks. Security of Internet of Things (IoT) has become a critical concern. The danger exposed by infested Internet-connected things not only affects the security of IoT, but also threatens the complete Internet ecosystem which can possibly exploit the vulnerable Things (smart devices) deployed as botnets. Mirai malware compromised the video surveillance devices and paralyzed Internet via distributed denial of service (DDoS) attacks. In the recent past, security attack vectors have evolved bothways, in terms of complexity and diversity. Hence, to identify and prevent or detect novel attacks, it is important to analyze techniques in IoT context."

4. Research Framework

Beyond the documents that I currently had access to, I did use the GSU library system to search databases for relevant content. I was looking for patterns of vulnerability and documented concerns surrounding IoT

security. Then taking the information, try to establish whether or not failures of IoT related data collection are being taken seriously. There are enough similarities within the Internet infrastructure that the scope of the research can be narrowed down to a more finite set of questions. Where attacks can come from? What type of data can be compromised? What is or has been done to remedy these issues?

Ultimately it would be impossible to cover every aspect of the cyber-security concerns within IoT in a single research paper. The end game of threat actors really has not changed, just the tools and methodologies.

Search terms like privacy, data harvesting, cyber-security led to a significant amount of data and thus made it difficult to narrow down the scope of the search. Ultimately, the decision was made to look at the NIST proposed standards and try to find supporting information of the standards actually being implemented.

5. Future Research Agenda

Future research into IoT cybersecurity may include topics such as intrusion detection of IoT. That area of study is interesting and as a matter of defense an ever changing subject. Additional pieces of study may include looking into IoT platforms. Perhaps do a compare and contrast as this is an unknown area to me.

6. Conclusion

With the discovery of NIST standards, it was a pleasant surprise to see that the fears listed in the introduction appear to have been addressed. The challenges at this point are, do manufacturers follow the guidance? We know that NIST is US guidance only and therefore we must be ever vigilant when choosing IoT devices. We need to ensure that source country is known as well as all that the IoT device collects, stores and transmits.

IoT is here to stay, the risks associated with these devices must also be clearly understood. Trust but verify, that is the way to evaluate products and not just blindly accept a manufacturers claims.

7. References

Basu, S. S., Tripathy, S., & Chowdhury, A. R. (2015). Design challenges and security issues in the Internet of Things. 2015 IEEE Region 10 Symposium. https://doi.org/10.1109/tensymp.2015.25

Batalla, J. M., Vasilakos, A., & Gajewski, M. (2018). Secure Smart Homes. ACM

Computing Surveys, 50(5), 1–32. https://doi.org/10.1145/3122816

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., … Scarfone, K. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. https://doi.org/10.6028/nist.ir.8228

Brill, H., & Jones, S. (2017). Little Things and Big Challenges: Information Privacy and the Internet of Things. SSRN Electronic Journal, 66:1183, 1183–1230. https://doi.org/10.2139/ssrn.3188958

Britton, K. (2016). Handling Privacy and Security in the Internet of Things.

Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). "Alexa, Can I Trust You?" Computer, 50(9), 100–104. https://doi.org/10.1109/mc.2017.3571053

Coulter, R., & Pan, L. (2018). Intelligent agents defending for an IoT world: A review. Computers & Security, 73, 439–458. https://doi.org/10.1016/j.cose.2017.11.014

Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1). https://doi.org/10.1186/s13677-018-0123-6

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020a). Foundational cybersecurity activities for IoT device manufacturers. https://doi.org/10.6028/nist.ir.8259

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020b). IoT device cybersecurity capability core baseline. https://doi.org/10.6028/nist.ir.8259a

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. IEEE Internet of Things Journal, 5(4), 2483–2495. https://doi.org/10.1109/jiot.2017.2767291

Lemos, R. (2016). IoT Devices Evolving Rapidly as Favorite DDoS Attack Tool, Experts Say. eWeek.

Megas, K. N., Fagan, M., & Lemire, D. (2021). Summary Report for the Virtual Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance. https://doi.org/10.6028/nist.ir.8379

Schneier, B. (2017). IoT Security: What's Plan B?

Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., … Elovici, Y. (2019). Security Testbed for Internet-of-Things Devices. IEEE Transactions on Reliability, 68(1), 23–44. https://doi.org/10.1109/tr.2018.2864536

Vaos, J., Agresti, B., & LaPlante, P. (n.d.). COLUMN: IT TRENDS A Closer Look at the IoT's "Things."

Vaos, J., & LaPlante, P. (2017). The IoT Blame Game.

Voas, J. M. (2016). Networks of "things." https://doi.org/10.6028/nist.sp.800-183

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Processing Magazine, 35(5), 41–49. https://doi.org/10.1109/msp.2018.2825478

Zhang, Y., Ma, X., Zhang, J., Hossain, M. S., Muhammad, G., & Amin, S. U. (2019). Edge Intelligence in the Cognitive Internet of Things: Improving Sensitivity and Interactivity. IEEE Network, 33(3), 58–64. https://doi.org/10.1109/mnet.2019.1800344