The Plant Ladder: An Automatic Plant Watering System
(Technical Topic)

Dissecting the Privacy Issues of Keeping Vocal Recordings with the Amazon Alexa
(STS Topic)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

CJ Rogers

Fall, 2020

Technical Project Team Members

Sonia Aggarwal

Brooke Bonfadini

Victoria Nilsson

Chloe Tran

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ____ Date __________

CJ Rogers

Approved ____ Date __________

Harry Powell, Professor and Associate Chair for Undergraduate Programs, Department of Electrical and Computer Engineering

Approved ____ Date __________

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

Since their inception 20 years ago, the popularity of Internet of Things (IoT) devices has skyrocketed. Mainly fueled by the growing availability of low-cost materials and low power computing methods, IoT has become a more practical and realistic alternative to many day-to-day operations. They have become very useful in the realms of Telehealth, Smart Cities, and simple home automation. Ranging from the smart speakers to door locks, over a billion devices are currently in use (Khan & Yuce, 2019). As these types of devices become more popular, the negative effects are becoming clearer. Connectivity, privacy, and security are some of the biggest issues that IoT developers deal with during design. As more devices come online the need for them to stay online becomes greater. If large scale systems suddenly go down, then major consequences would occur, and in circumstances of poor design could lead to the loss of human life. With so many people relying on these systems, sometimes holding personal information such as banking and medical records, security of that data is paramount. Since IoT devices are designed to be low memory and thus low power, there is a certain tradeoff between functionality and security that must be carefully considered. If security is added as an afterthought, the danger of having major security breaches is very likely. Even if data that is not of high importance is stolen from the device in question, the breach in privacy would still cause major harm due to a breach in trust with the supplying company. If these three items are not considered early in the design process in new devices, or patched in older devices, then they are likely going to fail on a larger scale and more often as the number of active devices grows. In order to improve the situation, this prospectus will discuss the design and implementation of one example of an IoT device, and examine the current state of one of the most widely used IoT devices, the Amazon Alexa, to understand its popularity as well as the privacy controversies it has encountered.

Technical Topic: The Plant Ladder: An Automatic Plant Watering System

Connectivity is one of the defining features of an IoT device. According to Dastjerdi and Buyya in *Internet of things: Principles and paradigms*, "IoT devices are generally characterized as small things in the real world with limited storage and processing capacity, which may not be capable of processing a complete computing activity by themselves." The feature of connectivity allows these small devices to work in conjunction with an online system that is more powerful to execute the functions that the small devices are not capable of. However, there is not just one way that these devices communicate. In *The Internet of Things*, Bunz and Meikle discuss the various ways that "it has become possible to link anything to networks," and that these devices "rely on many different communication protocols, such as Bluetooth, ZigBee, Near-Field Communication (NFC), Wi-Fi, Z-Wave, LoRa, Sigfox and others." With this many different types of communication methods, it starts to become clear why connectivity is such a crucial part of IoT devices. Many systems will need to account for more than one method of communication, and will need to know which one to use when in order to be most effective. This project specifically talks about one of those communication methods, Wi-Fi, in the context of farming. Farming is one field that has changed dramatically with the integration of IoT. Khan & Yuce describe how "IoT systems can make significant contributions to improve agricultural output, reduce crop failures," and more. By controlling "watering systems by measuring the soil moisture, temperature, humidity, sunlight and plant health through the sensory systems," (p. 10) an IoT device can make an extraordinary difference in a farm setting. These intelligent systems make human intervention less frequent, but more effective with the knowledge of exactly how the entire system is doing (Khan & Yuce, 2019). This project aims to accomplish the same tasks but on a much smaller scale.

The Automatic Plant Watering System my team is creating, named the "Plant Ladder", seeks to implement a system that will monitor the status of plants and act accordingly. Its main operations are to monitor the soil moisture, dispense water to a plant, turn lights on and off, measure water in a reservoir, and send data and critical system notifications to a user application using Wi-Fi. In order to do this the system has two kinds of sensors, two soil moisture sensors and a water level sensor. These sensors feed data to a low power microcontroller which handles all of the logic as to when water should be dispensed to a plant or when the threshold of water level in the reservoir is too low. Periodically, data from the microcontroller is sent to the end user application the process of which can be seen in Figure 1. The microcontroller is directly connected to a Wi-Fi module that handles all the wireless connections to the remote server that handles all of the data collection. The end user's application then uses the server database in order to populate it with data the user wants to see.

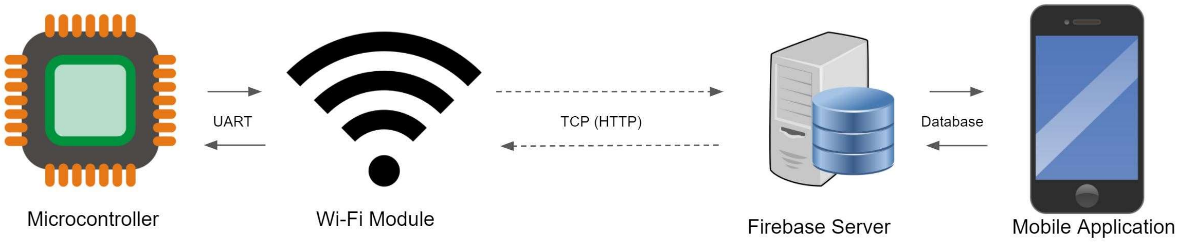

Figure 1: High Level Overview of the System. The microcontroller (MSP430) uses the UART communication protocol to send information to the Wi-Fi Module (CC3100). The Wi-Fi Module will then form the data from the MSP into an HTTP formatted request. The request is sent to the server which will be a holding zone for data until the application retrieves it and adds it to the application's database. (Created by Author)

One of the main design considerations made early in the project was how to connect the main watering system to the end user's application. Both Bluetooth and Wi-Fi were considered because they are well known and not hard for an end user to be able to understand and set up themselves. Ultimately, the decision was made to use Wi-Fi in order to align with the use case of monitoring the system from a distance. Bluetooth is limited by distance whereas Wi-Fi, when set up properly, the user would be able to access the system information no matter where they were. If the communication between the two sides of the project does not exist, then the application created would be useless. What defines an IoT system is the networking to other devices and general connectivity, so if the Wi-Fi functionality of the project is not completed, then the final product would not be considered an IoT device. While our project would decrease the need for human intervention and uses a small low powered device, if there is no level of networking or connectivity then the user would not get the benefits of a true IoT device. This project is just one example of how important connectivity is to an IoT device and why it is such a crucial consideration when it comes to designing a system such as this one.

STS Topic: Dissecting the Privacy Issues of Keeping Vocal Recordings with the Amazon Alexa

Internet of Things (IoT) devices, specifically smart speakers such as the Amazon Alexa, have been one of the main contributors to the boom in popularity. Hundreds of millions of Alexa devices alone are being used today. With an Alexa, normally comes a whole group of connected devices such as lights, thermostats, cameras, and more (Amazon, 2020). Since all these devices can be controlled by Alexa indirectly, it becomes much easier for a user to keep track of what is going on around the house and control it with only their voice, no need to move a muscle. The Alexa, however, is still not powerful enough to do any major tasks without the internet. All the computation and interpretations happen outside the device. As Lynskey (2020) says "as processing power increases, more tasks could be performed inside the device. But, of course, that would mean forfeiting that juicy, monetizable data." Since the devices are not powerful enough to do computations on their own, it gives Amazon a perfect opportunity to save and use the interactions with Alexa as data for their own means. And while it is not the most "pressing threat to privacy only because they are optional," (Lynskey, 2020) for those that do choose to use it, they incur a lot of risks that they should not have to in order to get the benefits of the device.

Amazon Alexa, and other voice assistants like Google Home, automatically "keeps a copy of everything Alexa records after it hears its name," so that they can "help train their artificial intelligences" (Fowler, 2019) but it has led to some privacy violations. Lynskey (2019) outlines three different cases where voice data was shared with those other than the user without consent:

1. "A judge in New Hampshire made headlines by ordering Amazon to submit Echo recordings of a double murder to investigators"
2. "Send recordings of private conversations to one of her husband's employees"
3. "was mistakenly sent about 1,700 audio files from someone else's Echo"

There was also a serious flaw in the system where "web services had bugs that a hacker could have exploited to grab a target's entire voice history" (Newman, 2020). While this issue has since been fixed, all these cases indicate that there are serious privacy and security issues when it comes to retaining voice records. While they may be useful for improving the product, "you cannot stop Amazon from making these recordings" (Fowler, 2019). There is a way to delete the history, but it is undocumented and hard to locate without looking it up. In order to restrict these types of data collection, legislation such as the Automatic Listening Exploitation Act has been introduced in certain US states that "penalize companies whose voice assistants and smart doorbells (such as Amazon's Ring) record conversations without permission" (Lynskey, 2019). While this does not solve the privacy problem, is it a step in the right direction so that the problem does not go unchecked.

In the way that the market has developed and the technology improved, there is an inherent tradeoff between user privacy and continuing improvement. While legislation should not be necessary from a pure ethical standpoint, the cases of breach in privacy introduced have shown that there is a need for it. The legislation is just one step that needs to be taken. Next is to examine what decisions have been made by designers of this technology, and do the benefits for the corporation outweigh the costs incurred by the users. The decision to place the improvement of technology before ensuring the privacy of the user shows a level of negligence that raises concern. While it is not on the same scale, mirrors decisions from *A statement by the American Society of Civil Engineering* regarding Hurricane Katrina. Similarly the "The ultimate goal of the risk communication program should be to produce an adequately informed and engaged public" (Andersen, 2006). In both cases, the truth of the situation is hidden from the very people it is meant to serve. Amazon needs to ensure the privacy of their voice logs until the eventual time when IoT devices will be able to handle everything on their own making many of the current privacy issues go away.

Conclusion

In order to get a better understanding of IoT devices, my part of the technical work will lead to a finished design and implementation of the automatic watering system, specifically the firmware and Wi-Fi connectivity feature. By making sure the connectivity is appropriately implemented, the importance of this feature as part of the team's final product would be very clear. It accounts for a large portion of the effort and thus is a large portion of the final automatic watering system.

My STS research will lead to an improved understanding of the benefits and costs of increased usage of IoT devices such as the Amazon Alexa. By examining its privacy issues with vocal recordings, the effect of privacy as a design consideration will be determined. Along with the effort in the technical project, this research will offer more insight into the possible uses of IoT and how to best ensure the safety of the user’s personal data.

References

Andersen, C. F., & al., e. (2006). *Hurricane Katrina: One year later: What must we do next? A statement by the American Society of Civil Engineering.* Reston, VA: American Society of Civil Engineers.

Bunz, M., & Meikle, G. (2018). *The Internet of Things.* Cambridge, England: Polity.

Dastjerdi, A. V., & Buyya, R. (2016). *Internet of things: Principles and paradigms.* Cambridge, MA: Morgan Kaufmann.

DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press: New Haven.

Fagbemi, D. D., Wheeler, D. M., & Wheeler, J. C. (2019). The IoT Architect's Guide to Attainable Security and Privacy. Auerbach Publishers, Incorporated: Milton.

Fowler, G. A. (2019, May 6). Alexa has been eavesdropping on you this whole time. *The Washington Post*.

Khan, J. Y., & Yuce, M. R. (2019). *Internet of Things (ioT): Systems and Applications.* Pan Stanford Publishing: Milton.

Lynskey, D. (2019, October 9). 'Alexa are you invading my privacy?' - the dark side of our voice assistants. *The Guardian*.

Neeley, K. A. (2008). Beyond inevitability: Emphasizing the role of intention and ethical responsibility in engineering design. In P. E. Vermaas, P. Kroes, A. Light, & S. A. Moore, *Philosophy and design: From engineering to architecture* (pp. 247-257). Heidelberg, Germany: Springer.

Newman, L. H. (2020, August 13). An Alexa Bug Could Have Exposed Your Voice History to Hackers. *WIRED*.