Internet of Things Security:

How to Keep IoT Devices Secure at Home

New Mexico

Supercomputing Challenge

Final Report

April 8, 2020

Team 25

Multi-Schools (MHS, EHS)

Team Number: 25

Team Members: Nancy Avila Do nancyavila.lpslover123@gmail.com, (505) 480-0385

Gwenevere Caouette gweneverecaouette@gmail.com, (505) 492-7788

Priscila Flores precelaflores10@gmail.com, (505) 359-9525

Kyreen White hellu.kittycat2004@gmail.com, (505) 347-8339

Teacher(s): Sharee Lunsford lunsford@aps.edu

Karen Glennon kglennon25@gmail.com

Sponsor: Karen Glennon kglennon25@gmail.com

Patty Meyer pmeyer2843@gmail.com

Areas of Science: Computer Science/Cyber Security

Table Of Contents

Executive Summary

Internet of things (IoTs) aren't difficult to understand, but it depends on what device you want to know about. We plan to figure out how easy it is to hack into a Google Home Mini. All IoT devices can be hacked differently and changes are depending on the hacker. If you connect to public Wi-Fi, you risk your information getting taken, unlike if you're connected to your own home Wi-Fi, then the hacker has to hack into your home Wi-Fi first in order to get to the rest of your home devices. When trying to protect your IoT devices, you can either call your provider or the company of that certain device.

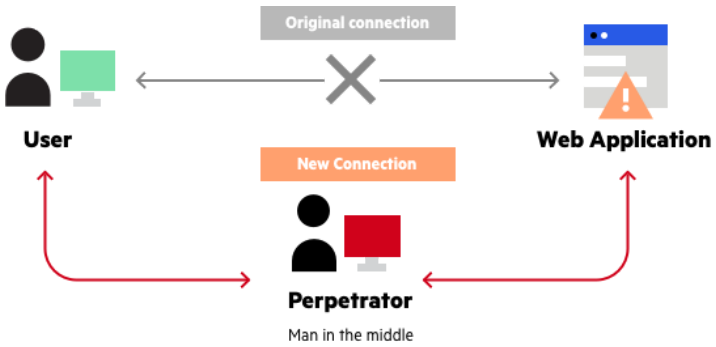
We have researched many devices, and we picked the Google Home Mini due to the fact that one of our members owns a Google Home. We have learned that with voice recognition there are two different settings. First, you can set the Google Home with just your voice so it only listens to your voice when recognized. Second, you choose not to set the voice recognition, and it will answer everyone. Also, with Google Home, it only responds to "Hey, Google " and "Okay, Google" and such settings cannot be changed. When using your Google Home Mini there is also an option switch to turn off your mic so it "can't hear you". We have also tested the Google Home with the setting that recognizes one person's voice, other voices are not recognized. However, when the three of us tested it (Nancy, Gwenevere, and Priscila) while Kyreen remained silent, Google Home responded to the three of us regardless of how low or high we would make our voice on the setting of 'set person's voice'. Because of the problem of voice detection, it creates a device that could be easy to infiltrate and could raise a big threat to the security of those who live in the household.

Definition of the Problem

Security has always been a top priority of society, but the advancement of technology has brought breaches to that security. Determining the different aspects of the hacker versus the person intervening with the internet is all done by the connection between the base of the hacker and the open minded person. We first started by figuring out what we wanted to prove. IoT

devices are hard to maintain and the security is conflicting due to how they are constructed. For example, when using public Wi-Fi; check in with the people that work there to make sure it's the correct one you want to use. However, useful technology may have been, many dilemmas have risen from the use of technology. Technology has advanced which has created situations where security breaches have occurred, also known as a vulnerable network. Technology has been used to inflict damage upon others in the form of hacking that can lead to exposing private information and discussions have started on how to keep areas secure. However, not every technological device is kept secure, if using Internet of Things (IoT) devices. For example, IoT devices are connected through Wi-Fi. Hackers have used the "Man in the Middle" (**Figure 1**) and "Evil Twin" (**Figure 2**) methods to acquire private information through a fake or intercepted Wi-Fi. If hackers can get internet data and get all private information, then it is possible to control your home network. How can individuals keep smart devices secure at home?

Figure 1: Man in the Middle



https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Man in the Middle is a hacking method. They intercept your connection to the internet and see everything you do before it reaches the internet.

Figure 2: Evil Twin

https://www.researchgate.net/figure/Illustration-of-an-Evil-Twin-Attack-The-attacker-can-successfully-lure-a-victim-into_fig5_321122614

Hackers create another Wi-Fi that is identical to the Wi-Fi available. Once clicked on, the hacker can see all the information from that device and takes their information through the 'evil twin' Wi-fi.

Figure 3: Table Differentiating Consumers

Consumers who are vulnerable to hackers:	Consumers who are not as vulnerable to hackers:
Own credit cards	Have a passphrase
Do not have passphrases	Do not sign into free unsecure Wi-Fi's
Own a social security number	Pay for a secure system
Does Not consecutively change passwords	Changes passwords conseculatively

Arranged By: Kyreen White

https://www.keyinfo.com/pros-and-cons-of-the-internet-of-things-iot/

https://www.pixelcrayons.com/blog/web/what-are-pros-and-cons-of-internet-of-things/

Problem Statement

IoT devices are not secure thus they are vulnerable to hackers. We are trying to keep IoT electronics as safe as we can through researching and fully understanding the hackers mindset and techniques. The biggest problem with IoT security is with hackers; due to the fact that IoT appliances are not secure they are vulnerable to being hacked. Hackers are resourceful, they are always trying to find the easiest way to access your information, so they choose the most vulnerable IoT device. Our problem is; how are we going to make IoT devices in our home safe so that the risk of a hacker getting into our devices is lower? In our code below we are modeling an IoT based network. With our code we are showing hackers hacking into your WiFi and using your IoT devices as a way to control your lights, your locks on your door, and cameras. They can access your IoT device through your WiFi and if you connect your IoT device

to your door lock and cameras, then they can turn your cameras off and unlock the door. When doing so, that creates a breach in the security of the device and the securty of those who live in the house.

Method

Currently the problem has not been solved. However, certain methods were used to get to where the team is now. Our team started with the first basic steps: 1) Answer Questions: What are IoT devices? How do they work? How do they connect? What devices are considered an IoT?
2) Hacking: How do hackers hack devices? What can be used to hack devices and to test their vulnerability? 3) What device type should be used? 4) Understand and gather information based on hacking and security reasons 5) Reach out to people who work with IoT devices and Cyber Security. When we got to step five, we had only gotten to the point of asking for their help; we have not yet worked with them in person. Research has been our main focus, however, we also want to learn how to hack our device and how to analyze its security. We will research ways to hack it through VirtualBox and Kali Linux as well as moving the code forward. VirtualBox is an open box software that allows the user to have a virtual model of a certain device. Kali Linux is a software that allows the user to use it as a digital forensic and penetration testing.

Throughout this project we will further it with the following steps: 1) VirtualBox and Kali Linux: Download and learn how to use the devices on the Google Home Mini 2) Research Google Home Mini Properties 3) Meetup and Discuss with Cyber Security and IoT experts 4) Finalize the code up to this point. With these steps it will help us get to where we want to be by the end of this year and where we want to start next year.

Code

This year our code was done on Netlogo as an experimental model. We decided that we wanted to show how easily someone can get your information from your IoT devices if they hack into the main server. The main server is the router where you get your Wi-Fi, it is a big gray turtle located in the middle of the interface. There will be a border around the main server made with patches, this will represent how there is a firewall around the main server to protect consumers

from hackers. We have blue circles that are turtles connected to our main server. These are representing the Google Home Mini you have connected to your Wi-Fi.

The shown connection is a green line, which shows how the connection to your Wi-Fi is not yet hacked into or seen as safe. The whole system is enclosed, just like how a house encloses all your devices. The hacker is a person outside of the "house." Once you press the hack button the hacker connects into the house's main server and hacks into your devices. The lines that were green, are now red. The red shows how the devices that were secure are now at risk and that your devices are no longer secure. There are a few buttons that are titled “Door” and “Lights”. It allows us to open the door or turn on the lights as if we were the hacker.

What we plan to do is show the security measures that the IoT devices have and how the hacker is able to use the products in the house. We want to add restrictions as to when the hacker can open the door or turn on/off the lights. The first condition is that the hacker has to be connected to Wi-Fi. Second, the hacker has to be able to infiltrate the Wi-Fi regardless if there is a strong or weak firewall. Lastly, once the hacker is connected, the security measures of the devices will try to cut the hacker out of the system.

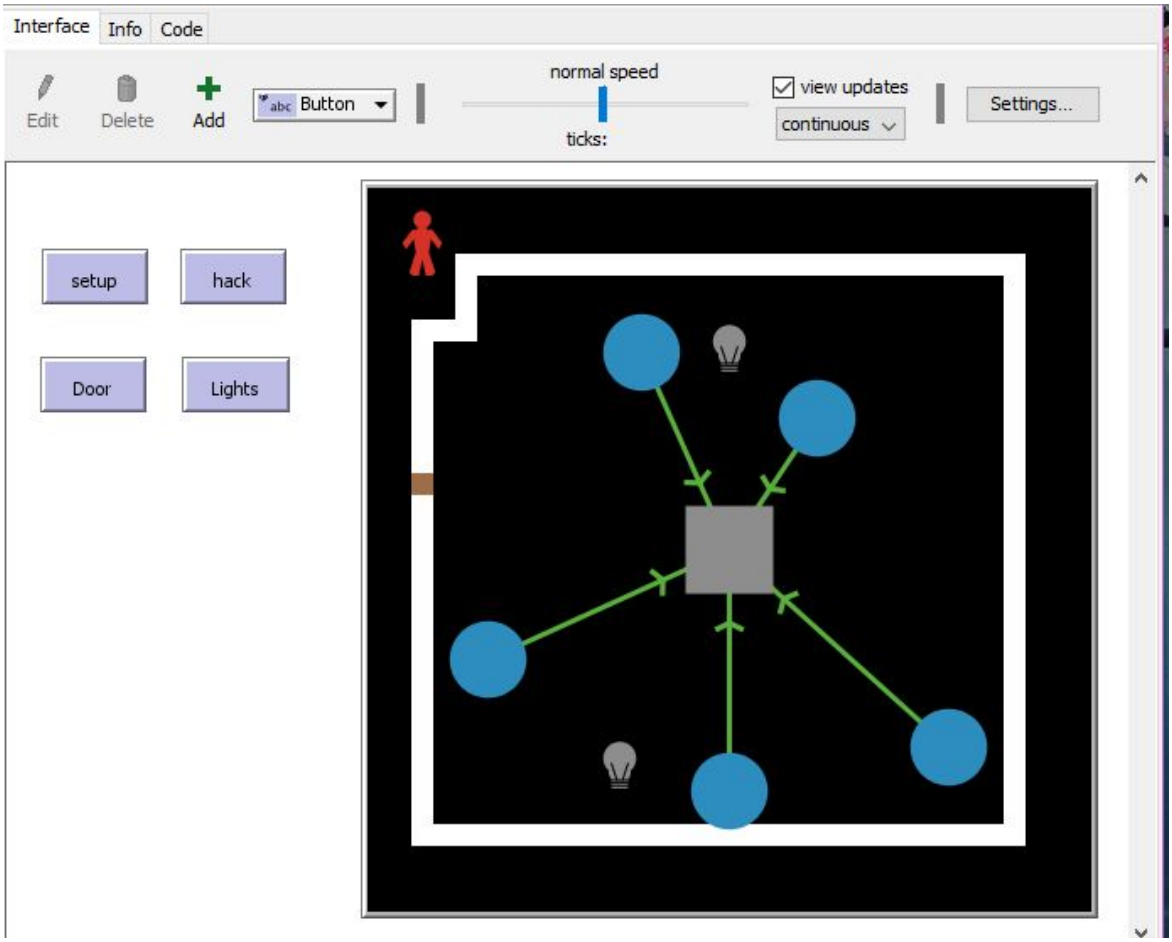
We also want our firewall to have two buttons, one that simulates a protected security and one that simulates a weak security. One button will have a fire wall that has one patch that works as an opening for the hacker to get into. The second button will have the firewall that entirely surrounds the Wi-Fi and it requires the hacker to break the firewall. We have only been able to create the Wi-Fi, the Google Home, the links, lights, door, house, and hackers.

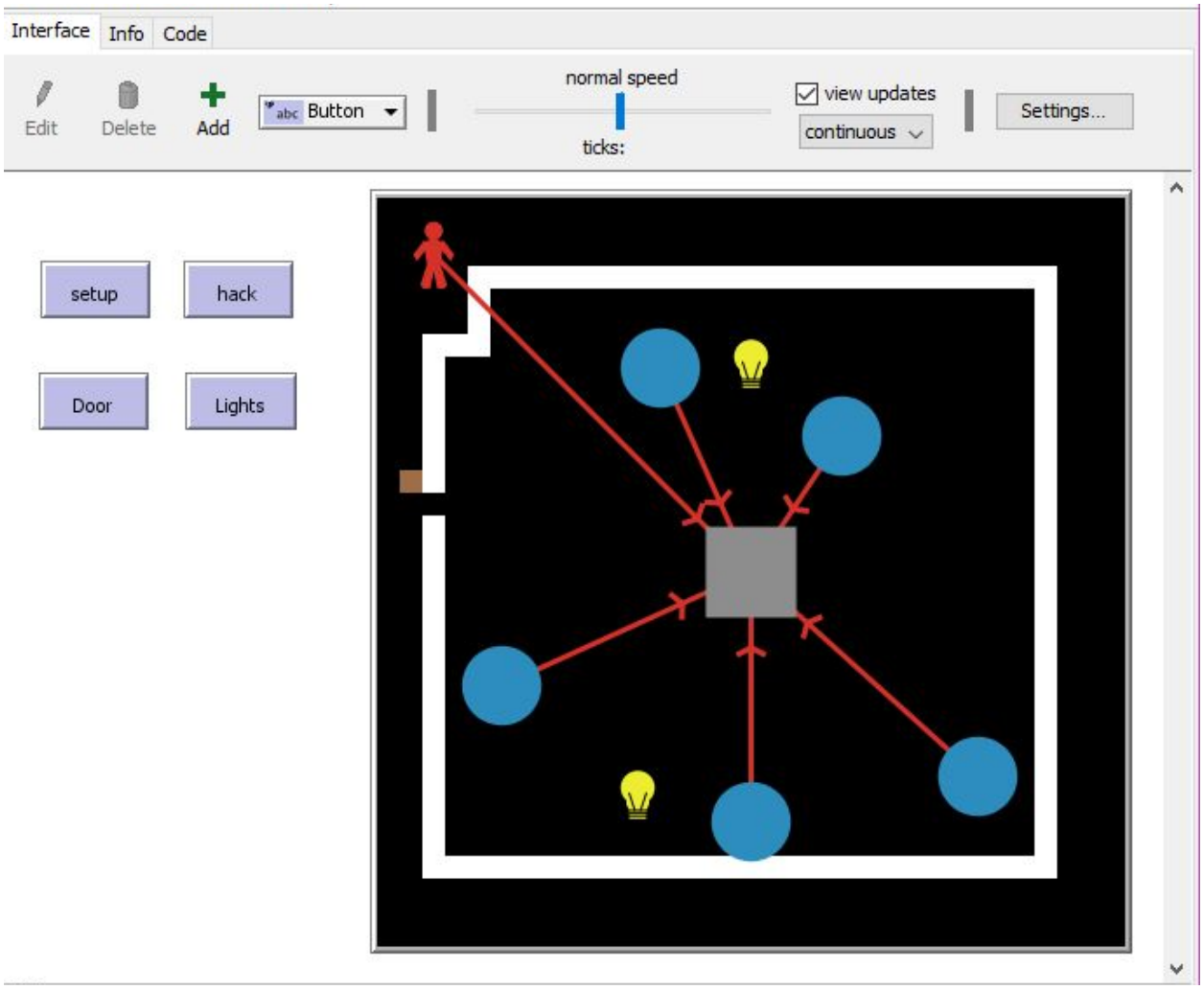
We have not yet been able to make the code simulate exactly as we described above however, we will continue to work on it next year. We have the hacker, the house, lights, door, and the “Google Home Minis” connected to the main server. When you press Hack, the hacker immediately hacks into the main server. For next year, we plan to further along the code for the following year, we are looking into other programs such as JavaScript. We want to see how it works and how we can make the code further progress in other systems and how they are different from Netlogo. We plan to extend our coding, as said above by coding in more precautions and protection for the main server.

The reason we did not finish our code this year is we did not want all our code to go to waste. We were told at our project evaluations in February that everything we did this year would not count for next year. As we want to continue on with our project next year, we want our code to count next year. Also, with what we want to do and to extend it, we are going to need a lot more time which we're getting from continuing our project.

Figure 4:

Interface




Interface
Info
Code
Edit
Delete
Add
Button
normal speed
ticks:
view updates
continuous
Settings...
setup
hack
Door
Lights

Code

```
breed [ Wi-Fi Wi-Fis]
breed [ Google Googles]
breed [ hacker hackers]
breed [ Lightbulb Lightbulbs]
to setup
  clear-all
   create-Wi-Fi 1 [
     set shape "square"
    set size 5
    set color grey
    set xcor 0
    set ycor 0

  ]
  create-Google 1 [
    set shape "circle"
    set size 3.5
    set color 515
    set xcor 4
    set ycor 6
  ]
  create-Google 1 [
    set shape "circle"
    set size 3.5
    set color 515
    set xcor 10
    set ycor -9
  ]
  create-Google 1 [
    set shape "circle"
    set size 3.5
    set color 515
    set xcor -11
    set ycor -5
  ]
  create-Google 1 [
    set shape "circle"
    set size 3.5
    set color 515
    set xcor -4
    set ycor 9
```

```
 ]
 create-Google 1 [
   set shape "circle"
   set size 3.5
   set color 515
   set xcor 0
   set ycor -11
 ]
 create-Lightbulb 1 [
   set shape "Lightbulb"
   set size 2.5
   set color gray
   set xcor 0
   set ycor 9
 ]
 create-Lightbulb 1 [
 set shape "Lightbulb"
 set size 2.5
 set color gray
 set xcor -5
 set ycor -10
 ]
 ask one-of patches [sprout-hacker 1]
 ask hacker [set shape "person"]
 ask hacker [set size 3]
 ask hacker [set color red]
 ask hacker [  set xcor -14
   set ycor 14
  ]
 Ask Google [
   create-links-to Wi-Fi
   ask links [set color 55]
   ask links [set thickness .25]
 ]
 ask patch 13 13 [
   set pcolor white ]
ask patch 12 13 [
   set pcolor white ]
ask patch 11 13 [
  set pcolor white ]
ask patch 10 13 [
  set pcolor white ]
ask patch 9 13 [
```

```
  set pcolor white ]
ask patch 8 13 [
  set pcolor white ]
ask patch 7 13 [
  set pcolor white]
ask patch 6 13 [
  set pcolor white ]
ask patch 5 13 [
  set pcolor white ]
ask patch 4 13 [
  set pcolor white ]
ask patch 3 13 [
  set pcolor white ]
ask patch 2 13 [
  set pcolor white ]
ask patch 1 13 [
  set pcolor white ]
ask patch 0 13 [
  set pcolor white ]
ask patch -1 13 [
  set pcolor white ]
ask patch -2 13 [
  set pcolor white ]
ask patch -3 13 [
  set pcolor white ]
ask patch -4 13 [
  set pcolor white ]
ask patch -5 13 [
  set pcolor white]
ask patch -6 13 [
  set pcolor white ]
ask patch -7 13 [
  set pcolor white ]
ask patch -8 13 [
  set pcolor white ]
ask patch -9 13 [
  set pcolor white ]
ask patch -10 13 [
  set pcolor white ]
ask patch -11 13 [
  set pcolor white ]
ask patch -12 13 [
  set pcolor white ]
```

```
ask patch -12 12 [
  set pcolor white ]
ask patch -12 11 [
  set pcolor white ]
ask patch -14 -13 [
  set pcolor white ]
ask patch -13 -13 [
  set pcolor white ]
ask patch -12 -13 [
  set pcolor white ]
ask patch -11 -13 [
    set pcolor white ]
ask patch -10 -13 [
    set pcolor white ]
ask patch -9 -13 [
    set pcolor white ]
ask patch -8 -13 [
    set pcolor white ]
ask patch -7 -13 [
    set pcolor white ]
ask patch -6 -13 [
    set pcolor white ]
ask patch -5 -13 [
    set pcolor white ]
ask patch -4 -13 [
    set pcolor white ]
ask patch -3 -13 [
    set pcolor white ]
ask patch -2 -13 [
    set pcolor white ]
ask patch -1 -13 [
    set pcolor white ]
ask patch -0 -13 [
    set pcolor white ]
ask patch 1 -13 [
    set pcolor white ]
ask patch 2 -13 [
    set pcolor white ]
ask patch 3 -13 [
    set pcolor white ]
ask patch 4 -13 [
    set pcolor white ]
ask patch 5 -13 [
```

```
    set pcolor white ]
ask patch 6 -13 [
    set pcolor white ]
ask patch 7 -13 [
    set pcolor white ]
ask patch 8 -13 [
    set pcolor white ]
ask patch 9 -13 [
    set pcolor white ]
  ask patch 10 -13 [
    set pcolor white ]
ask patch 11 -13 [
    set pcolor white ]
ask patch 12 -13 [
    set pcolor white ]
ask patch 13 -13 [
    set pcolor white ]
ask patch -14 -12 [
    set pcolor white ]
ask patch -14 -11 [
    set pcolor white ]
ask patch -14 -10 [
    set pcolor white ]
ask patch -14 -9 [
    set pcolor white ]
ask patch -14 -8 [
    set pcolor white ]
ask patch -14 -7 [
    set pcolor white ]
ask patch -14 -6 [
    set pcolor white ]
ask patch -14 -5 [
    set pcolor white ]
ask patch -14 -4 [
    set pcolor white ]
ask patch -14 -3 [
    set pcolor white ]
ask patch -14 -2 [
    set pcolor white ]
ask patch -14 -1 [
    set pcolor white ]
ask patch -14 0 [
    set pcolor white ]
```

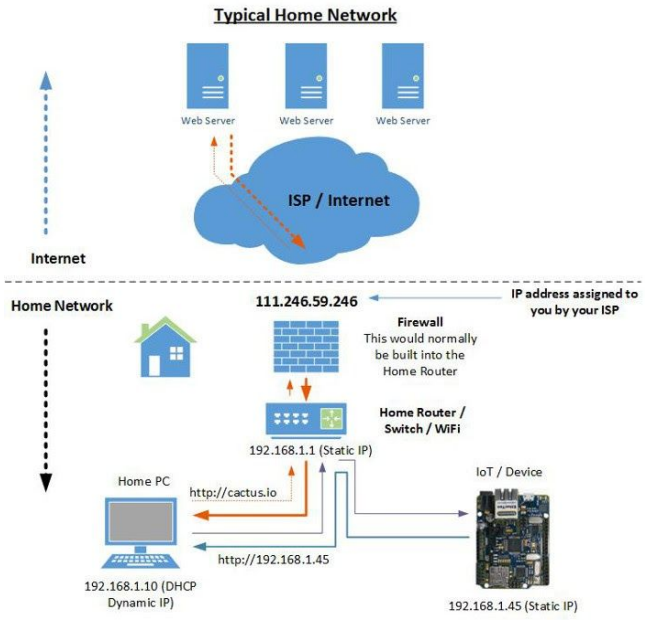
```
ask patch -14 1 [
   set pcolor white ]
ask patch -14 2 [
   set pcolor white ]
ask patch -14 3 [
   set pcolor brown ]
ask patch -14 4 [
   set pcolor white ]
ask patch -14 5 [
   set pcolor white ]
ask patch -14 6 [
   set pcolor white ]
ask patch -14 7 [
   set pcolor white ]
ask patch -14 8 [
   set pcolor white ]
ask patch -14 9 [
   set pcolor white ]
ask patch -14 10 [
   set pcolor white ]
ask patch -13 10 [
   set pcolor white ]
ask patch -12 10 [
   set pcolor white ]
ask patch 13 -12 [
   set pcolor white ]
ask patch 13 -11 [
   set pcolor white ]
ask patch 13 -10 [
   set pcolor white ]
ask patch 13 -9 [
   set pcolor white ]
ask patch 13 -8 [
   set pcolor white ]
ask patch 13 -7 [
   set pcolor white ]
ask patch 13 -6 [
   set pcolor white ]
ask patch 13 -5 [
   set pcolor white ]
ask patch 13 -4 [
   set pcolor white ]
ask patch 13 -3 [
```

```
    set pcolor white ]
ask patch 13 -2 [
    set pcolor white ]
ask patch 13 -1[
    set pcolor white ]
ask patch 13 0 [
    set pcolor white ]
ask patch 13 1 [
    set pcolor white ]
ask patch 13 2 [
    set pcolor white ]
ask patch 13 3 [
    set pcolor white ]
ask patch 13 4 [
    set pcolor white ]
ask patch 13 5 [
    set pcolor white ]
ask patch 13 6 [
    set pcolor white ]
ask patch 13 7 [
    set pcolor white ]
ask patch 13 8 [
    set pcolor white ]
ask patch 13 9 [
    set pcolor white ]
ask patch 13 10 [
    set pcolor white ]
ask patch 13 11 [
    set pcolor white ]
ask patch 13 12 [
    set pcolor white ]
End
to hack
  ask hacker [ create-links-to Wi-Fi
    ask links [set color red]
    ask links [ set thickness .25]
  ]
end
to Door
  ask patch -14 3 [
    set pcolor black]
  ask patch -15  4 [
    set pcolor brown ]
```

```
end
to Lights
  ask lightbulb [
    set color yellow ]
end
```

Figure 5: A Typical Home Network.

The basis for our Code.



http://cactus.io/tutorials/web/connect-iot-device-to-the-internet

Results

For this year's project we have not done enough tests that would get us the results needed for the project. As of right now the most that we have gotten is the research needed. We learned that IoT devices do not have the security that would keep them from being hacked. Some IoT devices do have security measures when it comes to opening a lock or a garage door, however, it seems that hackers do not have problems when hacking into the actual device. As of this moment we have only tested voice recognition between the four of us. We learned that because our voices were similar, the Google Home Mini would respond to us (Gwenevere, Priscila, and Nancy) as if we were our teammate Kyreen. Despite that, this does not prove the security measures with this test, for Google Home has a system preference where the IoT device allows you to choose between "Listen to my Voice Only" and "Listen to Anyone's Voice". Research and tests will continue next year as we continue this project.

Conclusion

So far we have done voice recognition and researched how IoTs work, through people who know more about them, videos, and websites. We will gain knowledge through books about IoT safety. We are going to be speaking with people who know more about IoT devices and cybersecurity. We will also work earnestly on our code, making sure it's where we want it to be. Security for the Google Home is the source of the problem that we are focusing on and we plan on going further with this project. With the feedback that we got from our judges during February evaluations. They asked us if we would continue next year because it's a meaningful topic to talk about in the future. We are planning to go into the public with a solution because not a lot of people have the protection they need.

Significant Achievements

Nancy Avila Do:

During this year's Supercomputing Challenge, there have been achievements that I was able to accomplish. I was able to lead this team in a way that we were able to do what we needed through due dates. I was especially proud of the work we have put on during this project. We have organized exactly what we wanted each week to end with and creating organization for this year's challenge was a huge help for us this year. Organization was a big thing that I wanted to include to this year's project, and because I was successfully able to do that with my teammates, it became one of my own achievements. I was also able to improve my public speaking skills and how to pick up wherever my teammates left off regardless of what my situations were, whether it was a personal matter or a public working matter. Another achievement was my code improvements. This year I was able to create the code that I wanted from what I saw when I was brainstorming its beginning steps. This year allowed me to accomplish goals that I never thought were possible to accomplish during this year's Challenge.

Gwenevere Caouette:

This Supercomputing Challenge year really allowed me to improve myself as a person. I was able to stay connected with my team and communicate to them even when things were hard. My most significant achievement was being able to learn different ways to code and to actually code. Every year I want to code, but this year I made it a priority and worked on it, even outside of meetings. I also saw how far we progressed as a team, we learned more and worked together better than ever. That was an achievement in itself.

Priscila Flores:

This is my first year in Supercomputing. I have been around Kyreen in Middle School and I always heard she went to Supercomputing, but I never thought of joining because I thought of myself to be too dull to be able to do this. I do not usually have problems with talking to people, but when it comes to presenting it makes me nervous, so I want to try to improve that as well. I

have learned that this is all about teamwork and making sure you can keep up with yourself and your teammates. I am looking forward to learning more about coding as well. I will, for sure, continue to be a part of this team.

Kyreen White:

This year, in the Supercomputing Challenge, has been amazing and I think we, as a team, have grown. I personally have a better understanding of how to work on a team. I have been involved with the project and deciding on our plans. When planning for our projects, I have been a big part. I am the researcher on the team and am always talking about the specifics. Everyone is always enthusiastic about finding new research, and I am always happy to help. The best thing our team does is work together. We are always ready for new challenges.

Acknowledgements

We want to acknowledge the following people:

Karen Glennon

We want to thank Mrs. Glennon for always helping us and encouraging us to keep going no matter what's thrown at us, whether it was a personal matter or a team matter. Mrs. Glennon, we are so thankful for all the help and time that you have dedicated to all of us here at Supercomputing Challenge. We are not sure what we would do without you here helping us and guiding us through these couple of years that we have been participating in the challenge. We are truly grateful for you. Thank you, for everything you have done for us.

Sharee Lunsford

We want to thank Ms.Lunsford for giving us advice and encouraging us, no matter what. We really appreciate you opening up your classroom for us to use, and offering us rides if we didn't have one. Thank you for pushing us further than ever, and we are really grateful that you have become one of our supporters. Thank you so much!

Patty Mayer

We want to thank Ms. Patty as she has always been sharing new ideas with us and added depth to our project. When we needed inspiration you were always there. Though sometimes we get off topic it is always great to talk to you. You always do the most interesting things and make our knowledge expand in just two hours. Anyway, thank you very very much for all your love and support.

Hussein Al Azzawi

We want to thank Hussein Al Azzawi for showing us around in the building to see the computer you guys have at UNM. Linux and the virtual playground will be a helpful resource to use. You

have been a big help to our project. We hope that we will be able to meet up with you next year to further our project. Thank you again for all your help.

Elizabeth Marie Kallman

Thank you for your email and reading over our project and giving us feedback. We know we have failed to meet, but your feedback has influenced our project. We are so thankful for your help in furthering our knowledge in this vast subject. Thank you very much. Thank you for giving us different resources to hack the Google Home Mini. We hope that we can meet with you in the future.

Scott Wilson

Thank you for your insightful information. You have been a great help especially since you wrote down a few resources for us to use for this project. We will continue to work with what you have given us. Thank you for all of your help and all the comments that you have given us to improve our project.

Varsha Dani

Thank you for being a project evaluator and thank you for your suggestions. Your questions during our presentation has helped us to further understand and guide our project to where we want it to be. Thank you for taking time out of your day to come and evaluate our project.

Drew Einhorn

We want to thank Mr. Einhorn for giving us advice and being our judge for the February evaluations. The advice you gave us pushed us further than ever and your guidnce helped us reevaluate our project. Thank you so much.

Rachel Goen

Thank you so much for the help you have given us with cyber security. You have been a big help so far although we have not been able to talk as much. Thank you for taking time out of your day to help us find resources with hacking.

References

1. (n.d.). Retrieved from https://commotionwireless.net/docs/cck/networking/learn-wireless-basics/.
2. Anatomy of An IoT Attack Retrieved from https://www.youtube.com/watch?v=GvLnb4YQHh0&t=1s
3. AARP Fraud Watch Network <AARP@email.aarp.org>
4. Bhagat, V. (2019, November 28). What are the Pros and Cons of the Internet of Things? Retrieved from https://www.pixelcrayons.com/blog/web/what-are-pros-and-cons-of-internet-of-things/.
5. Cisco IoT Threat Defense. (2019, October 17). Retrieved from https://www.cisco.com/c/en/us/solutions/security/iot-threat-defense/index.html?CAMPAIGN=SC-00%20Unaligned%20Security&Country_Site=us&POSITION=Social+Media&REFERRING_SITE=YOUTUBE&CREATIVE=Cisco.
6. Heubl, B. (2019, June 10). How to hack an IoT device. Retrieved from https://eandt.theiet.org/content/articles/2019/06/how-to-hack-an-iot-device.
7. How to Connect IoT Device to the Internet. (n.d.). Retrieved from http://cactus.io/tutorials/web/connect-iot-device-to-the-internet.
8. Internet of Things (IoT): Pros and Cons. (2018, February 27). Retrieved from https://www.keyinfo.com/pros-and-cons-of-the-internet-of-things-iot/.
9. Internet of Things Security Retrieved from https://www.youtube.com/watch?v=pGtnC1jKpMg
10. Porter, J. (2019, October 21). Security researchers expose new Alexa and Google Home vulnerabilities. Retrieved from https://www.theverge.com/2019/10/21/20924886/alexa-google-home-security-vulnerability-srlabs-phishing-eavesdropping.
11. Symanovich, S. (n.d.). What is a VPN? Retrieved from http://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html.

12. Swimming with Sharks - Security in the Internet of Things: Joshua Corman at TEDxNaperville
https://www.youtube.com/watch?v=rZ6xoAtdF3o