Keeping Personal Assistant Devices Secure at Home: The Google Home Mini (GHM)

New Mexico

Supercomputing Challenge

Final Report

April 7, 2021

Team 3

Multi-Schools (MHS, EHS)

Team Members:

Nancy Avila	navilad.735@gmail.com
Candis Canaday	candisc101@gmail.com
Gwenevere Caouette	gweneverecaouette@gmail.com
Kyreen White	hellu.kittycat2004@gmail.com

Teacher(s):

Ms. Lunsford	lunsford@aps.edu
Mrs. Glennon	kglennon25@gmail.com

Sponsor:

Mrs. Glennon	kglennon25@gmail.com
Patty Meyer	pmeyer2843@gmail.com

Mentor(s):

Brynn Charity

Richard Oliver

Thomas Robey

Areas of Science: Cyber Security (Computer Science)

Table of Contents

Executive Summary

This is the second year we have been working on this specific project. Our team has narrowed down from hacking IoT devices to the connection of the Google Home Mini (GHM) to the home network and the voice recognition security of the Google Home Mini. We focused on voice recognition and using synthetic voice to gain access to the personal information of the owner of the GHM.

The Google Home Mini responds to any person who says “Hey Google,” or “Okay Google,”. There are many different personalizations to certain commands; you can say “Hey Google, Good Morning” and set it to play certain music or tell you all your events for that day. Another command is “Okay Google, tell me when it is five” and they will set an alarm for 5:00 am. As said previously, the GHM will respond to anyone's voice (which is something we did not know last year), but that there are specific commands that are more personal to the owner of the device. We did two tests per GHM, with six trials. We focused on how a hacker could gain access to the GHM through voice recognition. We improved the code to have a synthetic voice that repeats the given phrase for our tests and are trying to make personalizations to the synthetic voice. The code was worked on in phases each phase being an improvement of the last. The first phase was to get the voice to say “Hey Google” inside the code itself. The second phase was to have the code generate a text box and allows us to insert any phrase we want. Each phase allowed us to get closer to using it for our tests with the device. Personalizing the synthetic voice to match one of our voices could make it possible that one can fool the GHM.

Problem Statement

The Google Home Mini, much like other IoT devices, is not a secure web-based device because it can control many different areas of your home at once. Through the focus of voice recognition and voice match which is a simple setup of saying a few phrases through the app, we have been able to control the google device. Once you set up the voice recognition, every time you speak to the GHM it should recognize you. To set up your voice match setting, you go through the app and select on your profile picture, there you go to assistant settings and scroll to voice match

which will tell you what to do from there to set up a voice match. More specifically, we set up a doctor's appointment on google calendar and set a reminder. Choosing these commands, through the GHM, is important because it requires the user to give authorization through voice recognition.

The research IoT devices' networks and the ways to hack into them. We found that there are even more simple ways to hack than we were thinking. For example, one can get personal information by asking the GHM "Okay Google, what am I up to today", and it will list out your whole schedule which is personal information and can be taken without fooling the device at all (if the voice match setting is on). Even just a simple phrase like setting a doctor's appointment could be used as a way of fooling through the device.

How are we going to keep consumers from being hacked through voice recognition?

Method

Throughout this project, we have worked to gather information and data that can further aid our project. We looked for information that could give us an idea of how the GHM works and how someone can fool it using voice recognition. During our project, we began exploring books, research, and testing. We researched IoT vulnerabilities, GHM vulnerabilities, firewalls, and GHM commands. After group research, the team was divided into two containing those of us who owned the GHM (Team 1) and those of us who did not own the device (Team 2). Team 1 would have Kyreen and Candis as the GHM testers. Their focus was to fool the GHM using voice recognition with the phrase "Hey/Okay Google, set a doctor's appointment for tomorrow at 4:00 pm." and "Hey/Okay Google, set a reminder for a doctor's appointment for 4:00 pm tomorrow." and record the response (on a table) to get a conclusion. Team 2 would have Nancy and Gwenevere work on the code and research. The two focused on researching the GHM and firewalls in-depth as well as creating a code that could be used with Team 1's testing. Team 2 focused on creating a code that used a synthetic voice that could repeat the same phrases that Team 1 focused on. Dividing the team into smaller teams has helped us gather more information and run tests during this year and has given us more opportunities to work in smaller groups for areas that we missed last year.

Code

This year, for our code, we decided to scrap last year's and redo everything. Last year, we used NetLogo to model how the GHM connects with different devices in the home network and how Man in the Middle works; however, this year, we decided to use Python to create a code that works with our project's goal. We wanted to originally update and fix last year's code, but because it was demonstrating how Man in the Middle works, it did not make sense to stick with it. Man in the middle is a type of hacking someone can do to get your information. This is when someone interrupts your wifi and anything you send to your wifi goes through the hacker. We met with multiple mentors to help us decide on our new code, mainly Mr. Tom Robey. Gwenevere and Mr. Tom met up almost every Tuesday to create our code. Our code this year is creating a Text to Synthesis Voice. While using Python and Jupyter Notebook, we started creating a synthetic voice that said one phrase. We then created a box that when entering a phrase, the voice repeats it back to you. The next step was to make the code say more than one sentence at a given time. We coded a program that, when entering a text file, will read it to you. We needed it to say paragraphs on command, so we created a code using Kivy in Jupyter Notebook and the program combined everything. It has a box on the left and a button on the other. When pressed, it repeats everything in the box.

In [*]:
```
import pyttsx3
text = "Ok Google"
engine = pyttsx3.init()
voices = engine.getProperty('voices')
engine.setProperty('voice', voices[0].id)
engine.say(text)
engine.runAndWait()
```

```
This is a voice command. Anything that is equal to the text, the computer will say it. The voice is a
robotic male voice, this can be changed later on depending on what you want.
```

In [*]:
```
import pyttsx3

def say(text) :
 engine = pyttsx3.init()
 voices = engine.getProperty('voices')
 engine.setProperty('voice', voices[0].id)
 engine.say(text)
 engine.runAndWait()

while True:
   text_to_say = input("Enter text to say : ")
```

```
Enter text to say :
```

This is what allows us to put anything in the enter to say box. The voice is suppose to put this in the box.

In [ ]:
```
import pyttsx3

with open('example.txt', 'r') as example_file:
    content = example_file.read()
    example_file.close()

def say(text) :
```

In [6]:
```
import pyttsx3

with open('random.txt', 'r') as random :
    content = random.read()
    random.close()

def say(text) :
    engine = pyttsx3.init()
    voices = engine.getProperty('voices')
    engine.setProperty('voice', voices[0].id)
    engine.say(text)
    engine.runAndWait()
    print(voices[0].id)

say(content)
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Speech\Voices\Tokens\TTS_MS_EN-US_DAVID_1
1.0
```

example file is where you can put any file you want and it be read to you.

In [4]:
```
from kivy.app import App
from kivy.uix.button import Button

class TestApp(App):
    def build(self):
        return Button(text='Hello World')

TestApp().run()
```

This should download an app into python. The app allows us to put any words and the computer soeak. Basically combining all our code previously and allowing us to use it to control the GHM.

In [ ]:
```
from kivy.config import Config
Config.set('kivy','keyboard_mode','systemanddock')
from kivy.app import App
from kivy.uix.button import Button
from kivy.uix.textinput import TextInput
from kivy.uix.boxlayout import BoxLayout
import pyttsx3

def say(text):
    engine = pyttsx3.init()
    voices = engine.getProperty('voices')
    engine.setProperty('voice', voices[0].id)
    engine.say(text)
    engine.runAndWait()


class SpeechSynthesisApp(App):
    def build(self):
        layout = BoxLayout()
        self.text_field = TextInput(hint_text='Enter Text here')
        button = Button(text="Perform Speech Synthesis", on_press=self.perform)
        layout.add_widget(self.text_field)
        layout.add_widget(button)
        return layout

    def perform(self,action):
        text = self.text_field.text
        say(text)


SpeechSynthesisApp().run()
```

Results

This year we have been testing the voice recognition on the Google Home Mini. We set up multiple commands which were recorded by five different people in an attempt to get the GHM to recognize an outsider's voice as the owner of the device. We ran the test on two different GHMs and got varying results. For the most part, the GHM would not allow unknown voices to complete commands that required voice recognition verification. However, on some occasions, it would allow a voice to complete commands multiple times. This is most likely due to the similarities between the two voices. In other instances, a voice would be picked up on the device but it was unable to understand the command even though it might hear it properly on a different trial of the same recording. We have also been developing code that we started to use in GHM tests. We have not yet been able to run a proper test with the code. What we have noticed so far is that the GHM will pick up on the "Okay Google" and "Hey Google" activation phrases.

Results of the Testing

Key

x	1	2	3
Owner's device. The owner did not do the testing.	The GHM completed the action.	The GHM did not complete the action	Other

Kyreen's Test 1

"Hey/Okay Google, set a doctor's appointment for tomorrow at 4:00 pm."

Speaker	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
Nancy	2	2	2	2	2	2
Candis	2	2	2	2	2	3
Gwen	2	2	2	1	2	2
Kyreen	x	x	x	x	x	x
Priscila	2	3	2	2	2	2

Kyreen's Test 2

"Hey/Okay Google, set a reminder for a doctor's appointment for 4:00 pm tomorrow."

Speaker	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
Nancy	2	2	2	2	2	2
Candis	2	2	2	2	2	2
Gwen	2	2	2	2	2	2
Kyreen	x	x	x	x	x	x
Priscila	2	2	2	2	2	2

Candis' Test 1

"Hey/Okay Google, set a doctor's appointment for tomorrow at 4:00 pm."

Speaker	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
Nancy	2	2	2	2	2	2
Candis	x	x	x	x	x	x
Gwen	2	2	2	2	2	2
Kyreen	2	2	2	2	2	2
Priscila	2	2	1	2	2	2

Candis' Test 2

"Hey/Okay Google, set a reminder for a doctor's appointment for 4:00 pm tomorrow."

Speaker	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
Nancy	3	3	2	3	3	3
Candis	x	x	x	x	x	x
Gwen	2	2	2	2	2	2
Kyreen	2	3	2	2	2	2
Priscila	3	2	1	2	1	1

Conclusion

After gathering information and data, we were able to understand that it is possible to fool the GHM with similar voices depending on the phrase. The tests allowed us to analyze the GHM and decide whether or not we could fool it; it allowed us to understand that the GHM can respond quickly. With a simple phrase using the control voice (the owner's voice), a recorded voice, and a synthetic voice, the GHM can follow through and do the given task. Yet, when using the three voice forms on a phrase that requires personal information and access, the GHM has trouble completing the task given. With further testing and code modification, one may be able to recreate the owner's voice frequency to potentially fool the GHM.

Significant Achievement

Nancy Avila Do:

This year was quite difficult; however, regardless of what was going on in the world, I was still able to work with my team to get things done. I was able to get my team to work on this project and persevere when we wanted to drop everything and stop. As a team leader, I was not sure how to lead my team during this time, but as I kept going, it was easier for me to lead and help my team. With the access of zoom, the team and I were able to meet with mentors. The added resources were something that did help us. I was able to help keep myself and the team on track, help with the code and created smaller teams to help us get more things done during this time. This year I was able to get more confidence when presenting online, leading online, and working more independently unlike in past years. Through the struggle, I was able to rise above it and make a solution out of it. It is odd to thank a pandemic for my achievements, but being able to work through those problems got me to where I am now. I am surprised by the fact that I was able to improve in my leading, presenting, researching, and coding skills. Even when I thought there was no way to improve during this time, I was still able to improve.

Candis Canaday:

With this year being the first time I competed in the Supercomputing Challenge, it is safe to say that it was a great learning experience. I learned about both STEM and about what I am capable of. Being in a pandemic made it a challenge to learn the new skills I would need to complete my work. With the help from my teammates, I was able to pick up on the skills easier than I had anticipated. Meeting frequently online was difficult at times, but it proved to be helpful. Even with the disadvantage of not being able to learn from my teammates in person, the online resources available allowed us to keep giving our all to the work we were doing.

Gwenevere Caouette:

My most significant achievement is the code this year. I was in charge of either scraping (which is the conclusion we ended up choosing) or updating the code we had at the beginning of the year. When we decided to start a new code, I had no idea where the project was going or what we were trying to prove. But through constant meetings with my team and Mrs.Glennon, we concluded that I needed help deciding the ultimate path and program we were going to use. We

met with Mr.Tom and he helped me learn Python, which was crazy and created a whole working code. Learning a new program, that I understand, is amazing. I am so proud of myself and the code we created.

Kyreen White:

Though it has been harder to stay in communication our team has done that pretty well. We have all known each other for a long time, so it is not hard for us to get a hold of each other. I feel that my most significant thing this year was completing the tests that we ran on the GHM. I felt like that was something that professionals did, and it felt so amazing to display my advanced understanding of our project. The idea that we have finished the tests and fully understood them was a big stepping stone for all of us. It just felt amazing. I am also proud of myself for not giving up and continuing with the Challenge this year as it was very hard to stay motivated this year. I had a very fun time this year nonetheless and I would like to thank my teammates for all of them being there for me and helping me understand my fidelity in the project.

Acknowledgments

We acknowledge the following people:

Tyler Brynn Charity

Thank you for your help with this project. Although we were not able to meet on a consistent schedule, you were able to help us with our project and made sure that we understood how a firewall worked and how we should run our voice recognition tests. Thank you for taking time out of your day to help us; we appreciate the time and advice that you have given us for this year's project.

Angela Chrisman

Thank you so much for giving us feedback on our February evaluations and giving us suggestions to move on from there. We have taken your suggestions and thoughts and used them. They have helped in moving on from that state of our project. Thank you again.

Karen Glennon

Thank you for helping us stay on track with the weekly Monday morning meetings. Your feedback allowed us to improve upon our work. Thank you for allowing us to create our best work.

Nick Kutac

Thank you so much for giving us great advice on our project during the February evaluations. We took all your comments and questions you had to further our project and make it better than we could have imagined.

Sharee Lunsford

Thank you so much for your help. Your guidance and advice have helped us with this year's project. Because this year has been so difficult, we are thankful for your guidance, presence, and advice during this year's project. Thank you for always being there when we need you.

Patty Meyer

Thank you so much for supporting our team. In a year that presented so many challenges, it was good to know that we had someone willing to help with whatever we needed. Thank you for your time, patience, and is the reason why we knew what project we wanted to do this year.

Richard Oliver

Thank you so much for helping out our team and helping us work through our difficulties involving the project. Thank you for recommending the ideas and giving us helpful feedback. We have enjoyed the time working with you and you giving us suggestions.

Thomas Robey

Thank you so much for your help with the code. Without you, our code would not have been where it is today. We would have been stuck and still afraid of trying new programs. Thank you for all the advice, we will be sure to use it for the rest of our time in Supercomputing.

References

Caines, M. (2019, January 10). How to Increase Firewall Protection. Retrieved November 30, 2020, from https://itstillworks.com/increase-firewall-protection-6909600.html

Can google home devices be hacked? (n.d.). Retrieved November 30, 2020, from https://support.google.com/assistant/thread/41773906?hl=en

Can Your Google Home or Google Nest Be Hacked? Here's How. (2020, October 03). Retrieved November 30, 2020, from https://robotpoweredhome.com/can-a-google-home-be-hacked/

Carey, J. (2019, October 21). Google Home and Amazon Echo apps just exposed a very dangerous security flaw. Retrieved November 30, 2020, from https://www.express.co.uk/life-style/science-technology/1193699/Google-Home-Amazon-Echo-security-flaw-exposed

A Complete Guide to Firewall: How to Build A Secure Networking System. (2020, November 13). Retrieved November 30, 2020, from https://www.softwaretestinghelp.com/firewall-security/

Features. (n.d.). Retrieved November 30, 2020, from https://www.hacksplaining.com/features

Gebhart, A. (n.d.). Everything you need to know about Google Home. Retrieved November 30, 2020, from https://www.cnet.com/how-to/everything-you-want-to-know-about-google-home/

Google Home Safety, Privacy and Security Tips. (2020, November 24). Retrieved November 30, 2020, from https://www.safety.com/google-home-safety/

Gupta, A. (2019). *The IoT hacker's handbook: A practical guide to hacking the Internet of Things*. Berkeley: Apress.

How Do Firewalls Work? . (2020, October 23). Retrieved November 30, 2020, from https://www.solarwindsmsp.com/blog/how-do-firewalls-work

James, L., & Luke James (8 Articles Published). (2018, November 26). 5 Essential Tips to Secure Your Google Home Device. Retrieved November 30, 2020, from https://www.makeuseof.com/tag/secure-google-home-tips/

Long, E. (2018, April 28). 5 Ways to Secure Your Google Home Device. Retrieved November 30, 2020, from https://www.tomsguide.com/us/secure-google-home,news-27076.html

NortonLifeLock, W. (n.d.). Can smart speakers be hacked? 10 tips to help stay secure. Retrieved November 30, 2020, from https://us.norton.com/internetsecurity-iot-can-smart-speakers-be-hacked.html

Porter, J. (2019, October 21). Security researchers expose new Alexa and Google Home vulnerabilities. Retrieved November 30, 2020, from https://www.theverge.com/2019/10/21/20924886/alexa-google-home-security-vulnerability-srlabs-phishing-eavesdropping

Ptacek, T. (2003, November 13). 10 tips for improving security inside the firewall. Retrieved November 30, 2020, from https://www.computerworld.com/article/2573934/10-tips-for-improving-security-inside-the-firewall.html

Security Tip (ST04-004). (n.d.). Retrieved November 30, 2020, from https://us-cert.cisa.gov/ncas/tips/ST04-004

Simic, S. (2020, September 30). 8 Types of Firewalls: Guide For IT Security Pros. Retrieved November 30, 2020, from https://phoenixnap.com/blog/types-of-firewalls

Smart Speakers Study (PETS20). (n.d.). Retrieved November 30, 2020, from https://moniotrlab.ccis.neu.edu/smart-speakers-study-pets20/

Spring, A., & Spring, T. (n.d.). DEF CON 2019: Researchers Demo Hacking Google Home for RCE. Retrieved November 30, 2020, from https://threatpost.com/def-con-2019-hacking-google-home/147170/

What is a Firewall? (2020, March 24). Retrieved November 30, 2020, from https://www.forcepoint.com/cyber-edu/firewall

What Is a Firewall? (2020, September 17). Retrieved November 30, 2020, from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Written by Alison Grace Johansen for NortonLifeLock. (n.d.). What is a firewall and do you need one? Retrieved November 30, 2020, from https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html