Celal Bayar University Journal of Science

Performing DoS Attacks on Bluetooth Devices Paired with Google Home Mini

Tuğrul Yüksel[1], Ömer Aydın[2*], Gökhan Dalkılıç[3]

[1]Dokuz Eylul University, Faculty of Engineering, Computer Engineering, İzmir Turkey
[2]Manisa Celal Bayar University, Faculty of Engineering, Electrical and Electronics Engineering, Manisa, Turkey
[3]Dokuz Eylul University, Faculty of Engineering, Computer Engineering, İzmir Turkey
*omer.aydin@deu.edu.tr
*Orcid: 0000-0002-7137-4881

Received: 7 January 2021
Accepted: 6 December 2022
DOI: 10.18466/cbayarfbe.856119

Abstract

In today’s technology world, virtual personal assistants (VPAs) have become very common and most people have started making their homes smart, using these VPAs. Although different companies have different assistants, Google Home Mini (GHM) is our focus in this paper. The first device, Google Home, was released in November 2016 and then GHM was released after a year, in October 2017. GHM has many features such as playing music, setting reminders, setting kitchen timers, and controlling smart home devices. Although GHM might be reliable against cyber-attacks, devices that are paired with GHM could be attacked and these cyber-attacks can lead to severe problems. Cyber-attack issues become more important to us, specifically if the devices controlled by GHM are vital devices such as ovens, fire alarms, and security cameras. In this article, we represent the denial of service (DoS) attacks applied against devices that are paired with GHM. In this study, Bluedoser, L2ping, and Bluetooth DoS script, which are software in the Kali Linux platform, were used to perform DoS attacks, and some devices were used such as GHM, headphones, and two speakers as victim devices. Successful results were observed on Bluetooth headphones.

Keywords: Bluetooth attacks, Denial of service attack, Google Home, Security, Network attacks, Virtual personal assistant.

1. Introduction

Using virtual personal assistants (VPAs) like Google Home Mini (GHM) to make our home smart is possible nowadays and many people do it successfully. As of 2017, newly developed VPAs such as GHM were presented to the market, so the capabilities and usage of virtual assistants have been started to expand rapidly. Smart home devices, GHM, and at least one device that is capable of running GHM applications are required basically for designing a smart home. Most of today's VPAs can interpret human voices and can respond via their defined voice. These kinds of VPAs are also able to understand lots of questions, manage smart devices connected to them. Moreover, they can manage basic operations such as calendars, alarms, and email checking. People use VPAs for different reasons. Some of them think that VPAs have a big role in easing their lives. Almost half of the users utilize features of a VPA such as browsing the web, weather forecasts, and music. Using VPA for online shopping and information is also possible.

Despite the advantages that a VPA provides to the user, there are serious security issues that are associated with using them. Although there is not much research on the use of VPAs, which is rapidly increasing, research continues in this area. The most important security issue is privacy. The questions we ask the VPA are stored on the servers and the responses we receive from the VPA are also sent to us by those servers. Although companies report that this data exchange remains confidential and the data is encrypted, our privacy may be compromised by another attacker during this data exchange between the server and the VPA.

1.1 Related Works

Zhang et al. (2018) reported a study that was a security analysis of popular VPAs and proved the vulnerability of VPAs against two new attacks [1]. They implemented two attacks that are called "voice squatting" and "voice masquerading", on GHM and Amazon Echo. These attacks focused on the way VPAs work or misconceptions of users about VPA functionalities. These two attacks were the proofs of a realistic threat to VPAs, as understood by their studies and the real-world attacks they performed. Finally, they implemented a context-sensitive detector to reduce the voice masquerading threat with a 95% precision.

Alrawi et al. examined possible security issues in 45 smart home applications and IoT devices [2]. They determined that most users were the reason for the security vulnerabilities. Users endanger their security for various reasons. In particular, they do this by using home assistants and IoT devices at different security levels. There has been research that offers a simple and effective solution for such security vulnerabilities. That solution is regulating the multiple IoT and Home Assistant usage and explaining the relational relationships to the users.

In another study, Park et al. (2018) discussed data storing and security methods of a GHM [3]. There are a lot of research projects that have been done on the other virtual personal assistants for digital investigations and the related article produces another one about a GHM. They separated the study into three main sections: the device, the mobile app, and the network and they analyzed the results obtained. In conclusion, they reported that the GHM does not store much data in the mobile app. The data that is exchanged across the GHM, mobile app and the Google cloud is analyzed by using Wireshark. The vulnerability tests on ajp13 port (one of the five ports of Google Home Mini) are proceeded and it is realized that it is not exploitable.

Caputo et al. (2020) dealt with that critical information about the habits of the users, which use VPA. The critical information can be leaked using the features of the encrypted traffic, such as the throughput, the size of protocol data units, or the IP addresses [4]. In a related study, they showed the risks of using VPA via models developed by using exploiting machine learning techniques to classify traffic and implemented privacy leaking attacks automatically.

Çepik et al. made attempts to attack the network time protocol and exploits were tested [5]. The attack was carried out on a wireless connection established between a Google Home Mini device and an Internet of things device. They examined secure communication between an IoT device and the GHM [6-8]. They tried to determine whether the Blynk (blynk.cc) application accesses time information via the simple network time protocol (SNTP) [9] from the time server. Thus, they tested the possibility that an attacker could obtain this information and interrupt the secure connection.

Giese and Noubir developed a set of forensic IoT techniques [10]. They applied these reverse engineering techniques to the hardware and software of the Amazon Echo Dot. They demonstrated that there is little protection of private user data. An attacker with physical access to such devices would be able to gain access to Wi-Fi credentials and can reach the sensitive information. They have shown that passwords and some sensitive information in the flash memory can be accessed even after the device is reset to factory settings. Finally, they proposed alternative secure designs and techniques to mitigate threats.

Yiğit tried to establish a secure connection using the AES algorithm between the NodeMCU and the Blynk in his study [11]. In this way, he aimed to prevent possible security vulnerabilities in the connection of the GHM with IoT devices.

There is increasing concern about the data collection and the security breaches of user privacy on devices like Amazon Echo and Google Home. Consumers sometimes unknowingly place too much trust in these devices. Ferraris et al. investigated the behavior of the devices such as Amazon Echo and Google Home in the smart home environment in terms of trust relationships [12]. As a result, they evaluated the effectiveness of the security controls provided and identified potentially related security issues. They defined a trust model to address the identified issues.

1.2 Aim and Contribution

Making a smart home or smart somewhere else is possible using GHM as told in the introduction section of the paper. This seems like a useful solution, but we have to be sure that the devices controlled via GHM are also secure. This paper focuses on the security of devices that are paired with the GHM via Bluetooth [13]. If the Bluetooth devices have some security weaknesses, the problem may become more vital. People can pair their vital devices such as an oven, security camera, or a fire alarm with GHM. The weakness(es) of those devices can cause irreversible damage and may harm people.

Our work aims to analyze the weaknesses of the devices and apply cyber-security attacks on them. To achieve our goal and simulate the attacks, the Ping of Death [14] attack, which is one of the DoS attacks, is used on the Kali Linux operating system. There are some customized tools for performing DoS attacks on the Kali Linux system. In our study, those tools are used for education research, and they shouldn't be used against someone else without permission. Attacking using those tools to someone is illegal and legal sanctions can be imposed on the attackers.

DoS attack is a type of cyber-attack in which a malicious attacker aims to render a computer or IoT device unavailable by interrupting the device's service [15]. DoS attack is launched from a single computer and the computer is also the attacker's device. DoS attacks harm by overwhelming a victim machine with requests until normal traffic is unable to be processed, resulting in a denial of service to users. In this study, useful tools of Kali Linux were used to send requests and packages.

In this paper, 2 Bluetooth speakers, 1 Bluetooth headphone, and GHM were used to achieve success. DoS attack was applied on those devices separately and different results were obtained. Three different Bluetooth devices were used as a victim because the results depend on the vulnerability of the devices. This study contributes to putting forth of risks of using a VPA and performing cyber-attacks using vulnerabilities of the devices. At the end of the study, results are presented and analyses are discussed. Attacks are performed on the victim devices one by one and software tools, which are used for cyber-attack, are applied on each victim device separately.

2. Materials

In our study, Bluetooth headphones, Bluetooth speakers, Kali Linux [16] operating system, and tools for DoS attack were used. GHM was used to pair victim devices via Bluetooth. Kali Linux, which includes tools for penetrating tests, was required as the operating system for performing DoS attacks. L2ping (linux.die.net/man/1/l2ping), Bluedoser (github.com/ Anlos0023/bluedoser) and Bluetooth DoS Script (github.com/crypt0b0y/bluetooth-dos-attack-script) are used for performing DoS attacks on victims. In this section, the GHM, Kali Linux, and tools for attacking are explained.

2.1. Google Home Mini

GHM, developed by Google; which allows us to turn our devices into smart devices in our home, office, or elsewhere; is an assistant that takes voice commands. GHM is connected to Google services over the Internet. Thanks to its microphone, it detects our voice commands and executes the commands. While devices that are on the same network as the GHM can be managed, we can also manage Bluetooth devices with the GHM.

There are lots of features such as turning lights on and off with the GHM, playing music by pairing our Spotify account with the GHM, managing our Netflix account with voice, sending voice messages, ordering food, calling by voice, creating alarms and reminders, managing smart home devices, etc. To use all these opportunities, it is enough to download the GHM application, complete the setup phase of the GHM, and make sure that the GHM is connected to the internet. After the setup phase, users can make the GHM listen to themselves saying "Hey Google" and can say the command they want to it.

Before using the GHM smart assistant, the device should be reset to factory settings by holding down the reset button on the back of the GHM. Using the Bluetooth service of the GHM, the setup phase is completed through the GHM application, and the device is connected to the Wi-Fi access point. Thus, the GHM becomes ready to access its services over the Internet. Finally, assistant settings can be changed through the device application, users can introduce their voice to the assistant and the GHM detects the voice that is introduced. Figure 1 simply describes the working principle system.

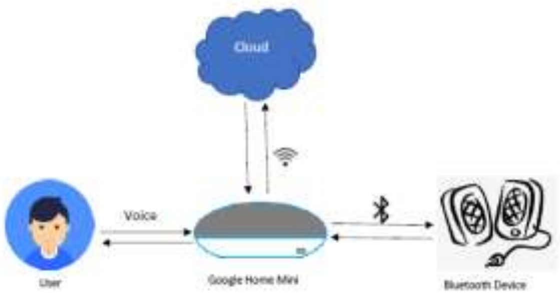


Figure 1. Google Home Mini system.

2.2. Kali Linux

Kali Linux is a Debian (en.wikipedia.org/wiki/Debian) based Linux operating system developed for penetration tests and security audits. Penetration tests are used to find, analyze and report vulnerabilities in systems. With a lot of tools and components for cybersecurity, Kali Linux is a widely used operating system for performing penetration tests. In this study, DoS attacks were performed using l2ping, Bluedoser, and Bluetooth DoS script tools on the Kali Linux system.

Bluez (bluez.org) is a library that provides the Bluetooth layer and protocol requirements necessary for us to use Bluetooth on our Kali Linux operating system. Bluez is developed in a modular structure which can support more than one Bluetooth adapter and also it contains many useful modules. Bluez, which can run on almost all Linux systems, can be downloaded using the “sudo apt-get install bluez” command.

Hcitool (linux.die.net/man/1/hcitool) contains many useful commands such as "dev", "scan", "inq". To reach all commands and detailed descriptions, the “hcitool -h” command can be used on the terminal. Finding the media access control (MAC) addresses of Bluetooth devices during our attacks is the first step to do before starting any operation. “hcitool scan” command finds those MAC addresses with their device names.

2.2.1. L2ping

L2ping allows us to send packets to Bluetooth devices. During performing l2ping, we need to determine some parameters such as "-i", "-s", "-f". The computer's Bluetooth adapter should be selected using the "-i" parameter. In this study, our Bluetooth adapter was hci0. By using the "-s" parameter, we can adjust the size of the packets to be sent. The target needs to be set by entering the victim's MAC address with the "-f" parameter.

2.2.2. Bluedoser

Bluedoser is a tool used to perform DoS attacks to disrupt the Bluetooth function. Bluedoser automatically tries to detect the surrounding Bluetooth devices and lists detected devices to the attacker with their MAC address. Then, the victim to be attacked is determined by finding from the list. Finally, a DoS attack can be initialized by entering the victim's MAC address into the interface.

Bluedoser performs a DoS attack using l2ping. The only difference is that Bluedoser attacks the victim using more than one thread instead of attacking by only one thread. That acts like sending packages from more than one terminal and the way used by Bluedoser disturbs the victim more periodically.

2.2.3. Bluetooth Dos Script

Bluetooth DoS script (BDS) is a script that works on only Linux systems and is used to perform Bluetooth DoS attacks. It is required by l2ping in the Kali Linux system to use BDS. The working principle of BDS is the same as Bluedoser, but the only difference is that BDS allows attackers to define thread count as a parameter. This parameter provides performing DoS attacks using a defined number of threads. Figure 2 explains how BDS uses it for attacking.

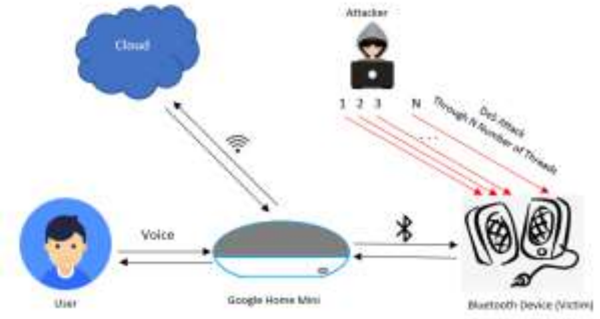


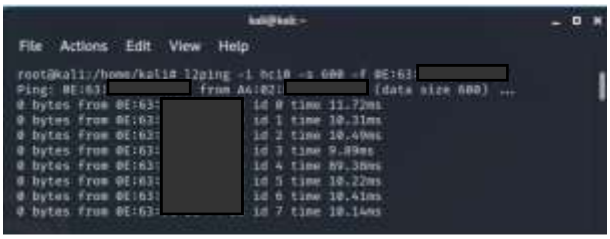
Figure 2. Performing DoS attack using BDS.

As soon as BDS attacks any unpaired Bluetooth device, it prevents other devices from connecting to the attacked victim device. For some devices that are not very secure, it may stop communicating with the corresponding device connected via Bluetooth. The security of the device to be attacked is the most important measure in the disconnection process via a DOS attack.

3. Proposed Work

First of all, the GHM application is downloaded to the device and the setup of the GHM proceeds through the application. After the GHM setup, we can integrate applications that support the GHM and many processes which we can do with our Gmail account. The GHM has a Bluetooth feature so that, we can pair Bluetooth devices in our house with the GHM and manage them by giving voice commands to the GHM. So, can we stop the services of these Bluetooth devices via DoS attacks? Especially if these Bluetooth devices have vital responsibilities such as fire alarms or security cameras, this issue becomes even more important for us. In this study, in addition to many studies on GHM security, we worked on DoS attacks against Bluetooth devices that are paired with the GHM. DoS attacks were applied based on the vulnerability of the Bluetooth devices. While the services of the non-secure devices were stopped, the Bluetooth connections of these devices with the GHM were also cut. In line with the results obtained, it is obvious that the devices to be connected with the GHM should also be secure.

Using l2ping, an attack was carried out on the Bluetooth headphone paired with the device. As the first step, as you can see in Figure 3, the parameters were adjusted, and then the attack was launched. Packets to be sent are set to 600 bytes, Bluetooth adapter and victim device MAC address are also set up. Only part of the MAC address can be read from Figure 3, the remaining is blackouted.

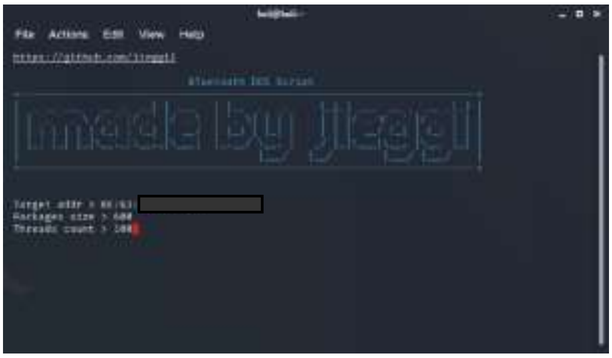


```
root@kali:/home/kali# l2ping -i hci0 -s 600 -f 0E:63:[redacted]
Ping: 0E:63:[redacted] from A4:02:[redacted] (data size 600) ...
0 bytes from 0E:63:[redacted] id 0 time 11.72ms
0 bytes from 0E:63:          id 1 time 10.31ms
0 bytes from 0E:63:          id 2 time 10.49ms
0 bytes from 0E:63:          id 3 time 9.89ms
0 bytes from 0E:63:          id 4 time 89.38ms
0 bytes from 0E:63:          id 5 time 10.22ms
0 bytes from 0E:63:          id 6 time 10.41ms
0 bytes from 0E:63:          id 7 time 10.14ms
```

Figure 3. L2ping

The victim device's MAC address was searched using Bluedoser's user interface. After determining the victim device, the related MAC address with the victim was set up as the parameter. Then DoS attack using Bluedoser was started on the Bluetooth headphone.

The user interface of BDS is as you can see in Figure 4. BDS requires Victim MAC address, package size, and several threads as parameters. After the DoS attack starts, packets of 600 bytes are sent to the victim over 100 different threads. The number of threads for achievement depends on the victim and this count may



```
https://github.com/jieggii
                 Bluetooth DOS Script
made by jieggii

Target addr > 88:63 [redacted]
Packages size > 600
Threads count > 100
```

Figure 4. The user interface of BDS.

change for different devices to be attacked. This optimal thread number was found by performing lots of attacks on the victim and observing those trials.

4. Results and Discussion

L2ping attack was failed even though the Bluetooth headphone accepted the packets. During the attack, music was playing over the headphone and service couldn't be denied. While sending the packages to the GHM, the GHM doesn’t accept the packages. When trying to send packages to the Bluetooth speakers, packages couldn't be received because the Bluetooth speaker already had a Bluetooth connection with the GHM.

In the attack on the Bluetooth connection between the GHM and the Bluetooth headphone using Bluedoser, expected success was not achieved and the Bluetooth connection could not be disconnected. The attack is performed on non-paired Bluetooth headphones and then it is tried to connect to the headphone via the GHM using Bluetooth. As a result, the GHM could not connect to the headphone.

In the attack on the Bluetooth connection between the GHM and the Bluetooth headphone using BDS, success was achieved and the Bluetooth connection was disconnected. Before the DoS attack, the GHM was playing music over the Bluetooth headphone as an output device. The GHM was changed the output device automatically after the DoS attack and it started to play music over itself. An optimal thread count was found for Bluetooth headphones and observations were plotted as a graph in Figure 5. Using 6 threads causes voice corruption on the headphone and using more than 6 threads provides disconnection of the Bluetooth connection between the headphone and the GHM. Using 7 threads offers the same result and using more than 7 threads is unnecessary, it just fatigues the attacker. The optimal thread number depends on the vulnerability of the Bluetooth device and this graph changes for different Bluetooth devices. Attacks should be performed again, and trials should be observed again to obtain a graph for another Bluetooth device.

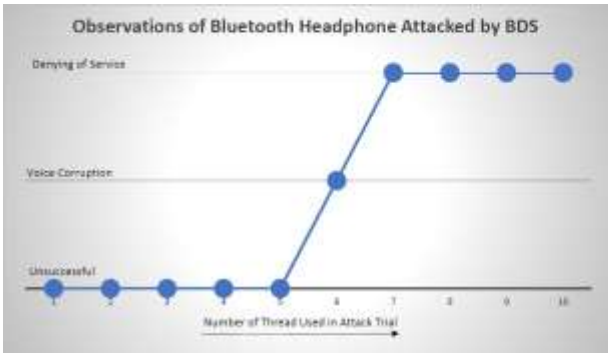


Figure 5. Optimal thread count for Bluetooth headphone.

We realized that we could not be successful in the DoS attack using l2ping, but we know that BDS uses l2ping and we succeeded in the DoS attack using BDS. This is because the BDS performs l2ping attacks over multiply defined threads and sends a suitable number of packages to the victim as much as possible to keep the victim busy. The optimal thread count parameter was found by observing different trials for Bluetooth headphones. Using at least 7 threads provided successful DoS attack results for our Bluetooth headphone.

5. Conclusion

In conclusion, attacks that were performed using l2ping, Bluedoser, and Bluetooth DoS script (BDS) were observed. No success was achieved using Bluedoser and l2ping against Bluetooth headphones and other Bluetooth speakers. Attack, which was performed using BDS against Bluetooth headphones, was able to disconnect Bluetooth service and victim headphone was denied of service.

We achieved success in performing a DoS attack on the device which supports more than one Bluetooth connection. Other devices didn't support more than one Bluetooth connection, so they didn't accept packets while the DoS attack has been performed. Future work aim is to find a way to perform DoS attacks on the other Bluetooth devices that don’t support more than one Bluetooth connection. It is required to find more vulnerabilities for those devices and to discover new techniques against security risks.

Author’s Contributions

Tuğrul Yüksel: Wrote the draft manuscript, prepare the system and made the experiments.
Ömer Aydın: Assisted in analysis on the structure, supervised the experiment’s progress, made result interpretation, helped in manuscript preparation, made the manuscript ready for the journal, took part in the journal submission and following the journal process.
Gökhan Dalkılıç: Served as a consultant in the execution of the whole process. He supervised the process of the preparation of the manuscript, made criticism and made the proof reading in language.

Ethics

There are no ethical issues after the publication of this manuscript.

References

[1]. Zhang, N, Mi, X, Feng, X, Wang, X, Tian, Y, Qian, F. 2018. Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home. https://arxiv.org/pdf/1805.01525.pdf

[2]. Alrawi, O, Lever, C, Antonakakis, M, Monrose, F. 2019 SoK: Security Evaluation of Home-Based IoT Deployments. IEEE Symposium on Security and Privacy. San Francisco, Ca. 20-22 May 2019. Doi:10.1109/SP.2019.00013

[3]. Park, M, James JI. 2018. Preliminary Study of a Google Home Mini. *Journal of Digital Forensics* 2018 June, 12(1). https://arxiv.org/pdf/2001.04574

[4]. Caputo, D, Verderame, L, Ranieri, A, Merlo, A, & Caviglione, L. 2020. Fine- hearing Google Home: why silence will not protect your privacy. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (JoWUA), 11(1), 35-53. https://doi.org/10.22667/JOWUA.2020.03.31.035

[5]. Çepik, H, Aydın, Ö, Dalkılıç, G. 2020. Security Vulnerability Assessment of Google Home Connection with an Internet of Things Device. 7th International Management Information Systems Conference. İzmir, Turkey. 09-11.12.2020.

[6]. Google Home specifications. Google Home Help. Google. Retrieved December 6, 2017.

[7]. Demmitt, J. 2015. "Google's Nest Labs plans top-secret project at new Seattle engineering center". Geekwire.

[8]. Statt, N, Bohn, D. 2019. Google Nest: Why Google finally embraced Nest as its smart home brand". The Verge. Retrieved October 9, 2019.

[9]. Mills, D. 1995. Simple network time protocol (SNTP). RFC 1769, University of Delaware.

[10]. Giese, D, Noubir, G. 2021. Amazon echo dot or the reverberating secrets of IoT devices. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 13-24.

[11]. Yiğit, E. 2021. Secure Connection between Google Home and IoT Device. *Journal of Emerging Computer Technologies*, 1(1), 18-20.

[12]. Ferraris, D, Bastos, D, Fernandez-Gago, C, El-Moussa, F. 2021. A trust model for popular smart home devices. *International Journal of Information Security*, 20(4), 571-587.

[13]. Sheppard, M. The Bluetooth basics.In: Bing B (ed) Wireless local area networks: the new wireless revolution, John Wiley & Sons, New York, 2002, pp 191-202.

[14]. Yihunie, F, Abdelfattah, E, Odeh, A. In Analysis of ping of death DoS and DDoS attacks, IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, USA, 2018, pp 1-4. IEEE.

[15]. Huegen, C. A. 1998. Network-Based Denial of Service Attacks. IEEE Transactions on Information Theory.

[16]. Singh, A. 2013. Instant Kali Linux. Packt Publishing Ltd.