ISSN : 1976-5304
https://kdfs.jams.or.kr

Preliminary Study of a Google Home Mini

Min Jin Park, Joshua I. James
Legal Informatics and Forensic Science Institute, Hallym University

구글 홈 미니에 대한 예비 연구

박 민 진, 조슈아 제임스
한림대학교 정보법과학연구소

ABSTRACT

Many artificial intelligence (AI) speakers have recently come to market. Beginning with Amazon Echo, many companies producing their own speaker technologies. Due to the limitations of technology, most speakers have similar functions, but the way of handling the data of each speaker is different. In the case of Amazon echo, the API of the cloud is open for any developers to develop their API. The Amazon Echo has been around for a while, and much research has been done on it. However, not much research has been done on Google Home Mini analysis for digital investigations. In this paper, we will conduct some initial research on the data storing and security methods of Google Home Mini.

Key Words : Digital Investigation, Google Home Mini, Smart Speaker, IoT, IoT Analysis, App Analysis

요 약

최근 많은 인공 지능 (AI) 스피커가 시장에 출시되었다. 아마존 에코를 시작으로 많은 회사에서 자체 스피커 기술을 생산한다. 기술의 한계로 인해 대부분의 스피커는 비슷한 기능을 가지고 있지만, 각 스피커의 데이터 처리 방법은 다르다. 아마존 에코의 경우, 모든 개발자가 API를 개발할 수 있도록 클라우드 API가 열려 있다. 아마존 에코는 긴 시간동안 사용되어 왔으며, 이에 대한 활발한 연구가 이루어졌다. 그러나, 디지털 조사를 위한 구글 홈 미니 분석 연구는 많지 않다. 본 논문에서는 구글 홈 미니의 데이터 저장 및 보안 방법에 대한 초기 조사를 수행한다.

주제어 : 디지털 조사, 구글 홈 미니, 스마트 스피커, IoT 분석, 앱 분석

Ⅰ. Introduction

Artificial Intelligence (AI) is a critical component of the Internet of Things (IoT). The cloud connects and controls various electronic devices based on the Internet. AI can control objects according to the surrounding environment. Also, self-learning is possible through natural language understanding and deep learning, and it is tailored to the convenience of users. Meanwhile, AI is an unshaped interface, so companies combine AI with device for commercializing. That is AI speaker. The AI speaker is a speaker with an AI secretary on the Bluetooth speaker. It can work with other AI devices and can be controlled by the voice. For international AI speakers include Amazon Echo, Google's Google Home and Google Home Mini and Apple HomePod. For domestic AI speakers include SK Telecom NUGU, KT GiGA Genie, Naver Clover and Kakao Kakao Mini. The AI speaker to be covered in this paper is the Google Home Mini made by Google. The Google Home Mini is a small

※ This work is funded by the KIAT(Korea Institute for Advancement of Technology) grant number(N0002260).
▪ Received 29 June 2019, Revised 05 September 2019, Accepted 18 September 2019
▪ 제1저자(First Author) : Min Jin Park (Email : minjinpark819@gmail.com)
▪ 교신저자(Corresponding Author) : Joshua Isaac James (Email : Joshua.I.James@hallym.ac.kr)

version of Google Home launched in October 2017 and launched in September 2018 in Korea. OS supports Android 5.0 or above, iOS 9.1 or above. To use the Google Home Mini, the user needs to sync it with the Google Home app, and the Google assistant will work when user registers and Wi-Fi certified in user app [8]. There has not been much research on the Google Home Mini compared to the Amazon Echo. In this paper, try to analyze Google Home Mini, its data storing system and security system. Research subjects include Google Home Mini, Google Home App, network, and local API. Then, with the data obtained, will be solved in terms of digital forensic perspective.

Ⅱ.Background Research

Chung [2] presented a cloud acquisition tool for IoT environments, which is called CIFT(Cloud-based IoT Forensic). They tested it for about two months. For the quality of the test, they focused on certain products, web browsers and used python. Through the test, they got unofficial Alexa APIs, native artefacts – user accounts, Alexa-enabled devices and saved Wi-Fi settings, client-centric artefacts and web cache. Especially for the web cache for Android and Chrome, it seems as though the data has the potential to be useful digital evidence as it helped to expect the user's action. Though the paper, they focused on the findings and proof-of-concept tool to be useful for researchers who work on Amazon Alexa in digital forensic investigation view. In the paper, it will be useful to mention what kind of comments they gave, how much data left.

Clinton [12] tested Amazon echo's system on privacy and vulnerabilities for security. By tearing down the speaker, we tried to exploit the echo hardware system. The paper found three primary methods to access to the speaker, which are the SD card pinout, an eMMC style root, and JTAG. It means Amazon echo is vulnerable for the physical attack, which means people can access to the speaker and get the data out from the speaker, and the privacy of the user is also in danger. Thus, the paper suggests being aware of these kinds of matters to protect the data. Currently released AI speakers are hard to connect physically. Therefore, it would be unlikely to happen.

Wohlwend [10] discusses Amazon Alexa and echo system structure, security policy and security test for the Echo. The paper focuses on three main goals for security, which are confidentiality, integrity, and availability. Then through the four-security testing – sound, network, direct API, and third-party skills – they find that Amazon echo stores data based on the Amazon cloud server and the device resist an attack of network and API. Then imply the third-party skills can be a vulnerability. It would be good if the paper talks more detail about the API based attack and give a try on third-party skills not only mentioning on the paper.

A 2018 article [7] describes how Google voice technology works in digital forensics. 'OK, Google' can be used to unlock mobile locks. If you have only the voice file of the suspect, you can unlock the phone and extract the data. In other words, the suspect's voice can be used to find the suspect's mobile device. Also, it can be applied to other smart devices using the Google assistant. The Google Home Mini can also wake up the device with 'OK Google' or 'Hey Google', and some features require voice verification. This means that if the suspect is a user of the Google Home Mini, the suspect's voice can tell whether the device is being used or not, and if the Google Home Mini is connected to another smart device, also can find some data of the suspect.

Hyde [13] analyzed Amazon echo, and Amazon echo dot devices itself, Kasa and Alexa mobile app, network, connected devices Amazon echo has SanDisk SDIN7DP2-4G, ISP pin is out. Amazon Echo Dot has different eMMC on each board. ISP pin is also out. Through the imaging, they found Wi-Fi connections, device information log, registration information from the device. In the app, they found, some databases and in the web application, they got URL of calling and messaging. Also, for the APIs, the cards, device, Wi-Fi, Smart Home devices, Activities were found. In the Kasa, which was the TP-Link smart devices mobile app, some critical data were found such as account, password and location. They focused on what kind of data was stored and where the data was stored.

Dipert [3] explains the inside of Google Home Mini by tear down. Inside of the device, audio amplifier, metal shield with a combination of Marvell's 88DE3006-BTK2 system SoC, Toshiba NAND flash memory, two embedded antennas, SK Hynix 4GB DDR3L SDRAM, microphones and manufacturing code sticker are found. In the papers, expect the same result as this blog shows and will be a more detailed explanation.

Moore [14] investigated about Google speakers based on the several investigative questions. He analyzed Google Home app with mobile phone, device itself using software tools and chip off and lastly, cloud service. From the phone, google account information, device location, cloud device ID and wifi password are been found. By examining the internals of the speaker, open ports, GET/POST requests, and Bluetooth information that is connected to the device such as MAC address, device name and date that has been connected. From the chip off, Google Home Mini has Toshiba TC58NVG1S3HBA16 256 MB NAND flash and use BGA 67 Socket, NAND Flash Chip Reader (Dataman) to read the data inside of the chip. From the dump, Bluetooth device information and Google account. For cloud acquisition, mainly used Google's 'My Activity' and Google Takeout. Through acquisition, not all but some given commands and answers were found. for the future work, parse Google Home file system, decoding of the proto file, iOS app examination and calling feature.

Ⅲ.Research Problem and Methodology

To date, very few works have looked at the Google Home Mini (GHM) from a digital investigation perspective. This work is an initial analysis of the locations and types of data related to the Google Home Mini, and is meant to be a starting point for future data acquisition studies. In this work, we separate the study into three main sections: the device, the mobile app and the network. Based on our past experiences, each of these locations provide different – but related – data that may be of evidential value.

We used Google Home Mini's built-in functions and direct interaction to generate user-related data. Commands were given directly to the Google Home Mini (serial number: 7B28L5NRWF) as well as via the mobile phone application (Galaxy note 4, SM-N910S, Android version 6.0.1). For this research, Korean and English were used to give commands. After the function test, chip-off was used to acquire additional embedded device data. After the chip off, the chip was imaged using Hancom GMD MD-series acquisition software.

Google has a mobile app called 'Google home'. The app version we used was 2.9.40.16. A user can give a command from the phone by speaking or typing. Also, the user can control the device in the app. To extract the data that is stored in the app, the ES File Explorer has been used. ES File Explorer is a free and featured file (application, document and multimedia) manager for local and network use. The version is 4.1.9.9.21. For the analysis, the phone (Galaxy Note4, SM-N910S) and laptop (Samsung, NT905S3G-KSQB) have been used. First, it generates data using the app. Then in the ES File Explorer, check whether the phone is rooted. Second, follow the path: device/data/data/Chromecast. Third, copy the Chromecast folder and paste in the internal storage. Then connect the phone to the laptop using a USB cable to extract the Chromcast folder. After all these steps, in this research, use Autopsy (version 4.10) to analyze the data. Add folder as Logical file.

In the network analysis, use Wireshark (version 3.0.0) and Zenmap (version7.7.0) to acquire the data. Figure 1. shows how the network has connected for the test. Google Home Mini and the mobile phone are connected to the laptop – the laptop works as an access point using its hotspot – and the laptop is connected to the internet and internet connects to the Google cloud.

We use the GUI version of Nmap, Zenmap, to look for open ports in the speaker's IP address. Use Telnet to see if the ports are listening. The test the vulnerability according to the usage of each port. Vulnerability testing uses Metasploit, Heartbleed and Openssl with Kali Linux. After that, uses Burp suite (v1.7.36) and Postman to acquire the data. In the Burp Suite, under proxy, add the laptop IP address and port 8080 and in the mobile phone Wi-Fi advanced setting, set proxy manual and port 8080. Then it intercepts the network of the speaker that talks to the phone through the laptop.

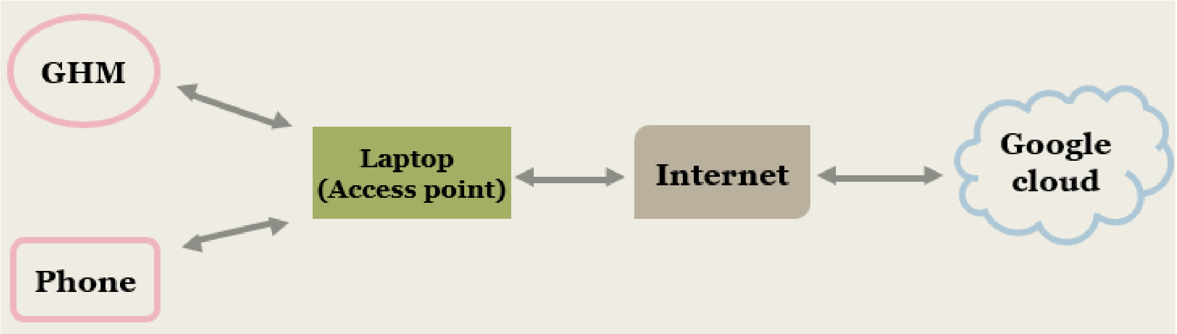


그림 1 디바이스, 모바일 앱 그리고 네트워크 데이터 수집을 위한 구글 홈 미니 네트워크 셋업.
Fig. 1. Google Home Mini network setup for device, mobile app and network data collection.

Ⅳ. Data collection and Analysis

This section covers different types of analysis we conducted on the Google Home Mini hardware and software with a focus on the mobile app analysis.

1. Google Home Mini Hardware

The Google Home Mini measures 98mm in diameter, 42mm in height and weight 173g. The colours are chalk, charcoal, coral-google store exclusive, and durable fabric material on the top. The Wi-Fi network supports 802.11b/g/n/ac (2.4 GHz/5 GHz) and features 4.1 Bluetooth. There is a microphone on/off switch and a micro-USB power connector on the back and a reset button right below the power connector.

2. Google Home Mini Functions

To use the functions, the user should say wake-up words are 'Hey, google' and 'Ok, google'. About 20 languages are available. If the user talks in English, the speaker responses in English. If the user talks in Korean, the speaker responses in Korean. Also, it provides information related to the language. There are many functions. It is similar to other speakers – for example, weather, alarm, news, traffic, and more. Among the functions, there are two functions which are 'Routine' and 'Remembering Things'. User can make a routine command to suit their lifestyle. For example, if the user says 'Bedtime, the speaker tells tomorrow's weather, tomorrow's first calendar event and ask what time the alarm should be set for then play sleep sounds. It will be a good way to know user behaviour. For 'Remembering Things', once the user gives the command 'remember that my key is on the desk next to the door', Google Home Mini accept the command, and when a user asks for the key, it tells where the key is. It will be useful to find something about the user.

3. App Analysis

Table 1 shows data and locations from the Google Home app on the mobile phone. Some tokens, account ID, the nickname of the device, address of the speaker, app version, port, phone IP address and Wi-Fi name and password list. For the Wi-Fi and password list, the phone has been connected to three different networks. Neo_house6 is the actual network router, and DESKTOP-ENIL7DS is a hotspot from the laptop. Both laptops were connected to the router and hotspot.

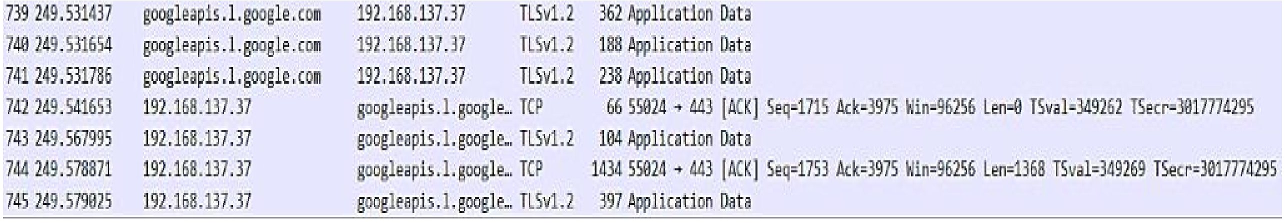
With the information from the app, it can be used when the users deny that they have never use the speaker or they do not have one. The user ID and location will verify and identify where the user is and was. Also, with the tokens, extract the data from the cloud is available. Also, Wi-Fi tells the connection between the user and the speaker.

표 2 구글 홈 미니 모바일 앱 분석에서 발견된 잠재적 증거 데이터
Table 1. Potential evidential data found from the Google Home Mini Mobile App Analysis

Location	Data
/LogicalFileSet1/com.google.android.apps.chromecast.app/shared_prefs/com.google.android.gms.appid.xml	LastToken appVersion
/LogicalFileSet1/com.google.android.apps.chromecast.app/shared_prefs/com.google.android.apps.chromecast.app_preferences_no_backup.xml	lastRefreshTime selected_routine_device_id ph_server_token gcmIdToken 61 Sakju-ro, Gyo-dong, Chuncheon, Gangwon-do, South Korea Longitude/ latitude home_graph_last_refreshed_simonhallym@gmail.com addressLine2 Chuncheon, Gangwon-do 200-060 current_account_name simonhallym@gmail.com Wi-Fi name and password list [{&quot;n&quot;:&quot;neo_house6&quot;,&quot;p&quot;:&quot;********&quot;,&quot;s&quot;:2},{&quot;n&quot;:&quot;DESKTOP-ENIL7DS 3926&quot;,&quot;p&quot;:&quot;dkssudgktpdy!!&quot;,&quot;s&quot;:1},{&quot;n&quot;:&quot;me&quot;,&quot;p&quot;:&quot;********&quot;,&quot;s&quot;:2}] current_home_id_simonhallym@gmail.com addressLine 61 Gyo-dong
/LogicalFileSet1/com.google.android.apps.chromecast.app/shared_prefs/com.google.android.apps.chromecast.app_preferences.xml	live_card_consistency_token com.google.h.b.d.a.w@7bc6f dismissedActionChipSetupDevicesFA:8F:CA:98:A5:5 setup-salt e3452b4b-9fd6-42b6-8e47-e71bc8dd0741
/LogicalFileSet1/com.google.android.apps.chromecast.app/cache/cronet_http_cache/prefs/local_prefs.json	servers:https://googlehomefoyer-pa.googleapis.com expiration:13200914931582426 port:443 address:192.168.166.11
/LogicalFileSet1/com.google.android.apps.chromecast.app/files/home_graph_c2ltb25oYWxseW1AZ21haWwuY29t.proto	OfficeZeLIFS simonhallym@gmail.com 216-33 Gyo-dong, Chuncheon, Gangwon-do, South Korea bettyhallym@gmail.com2 google.com:api-project-498579633514 5759C8B0CEAFB4B8D438569D3288716F: 41d28897-d2b4-4d80-bc26-de7057ec36b6 google.com:api-project-498579633514 5759C8B0CEAFB4B8D438569D3288716F

4. Network Analysis

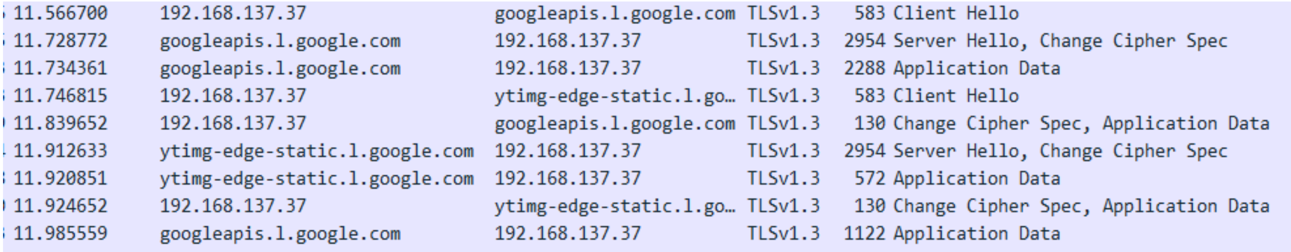
We used Wireshark to capture the network traffic between the access point, the Google Home Mini and the mobile device running the GHM app.



```
739 249.531437   googleapis.l.google.com   192.168.137.37          TLSv1.2   362 Application Data
740 249.531654   googleapis.l.google.com   192.168.137.37          TLSv1.2   188 Application Data
741 249.531786   googleapis.l.google.com   192.168.137.37          TLSv1.2   238 Application Data
742 249.541653   192.168.137.37            googleapis.l.google…    TCP        66 55024 → 443 [ACK] Seq=1715 Ack=3975 Win=96256 Len=0 TSval=349262 TSecr=3017774295
743 249.567995   192.168.137.37            googleapis.l.google…    TLSv1.2   104 Application Data
744 249.578871   192.168.137.37            googleapis.l.google…    TCP      1434 55024 → 443 [ACK] Seq=1753 Ack=3975 Win=96256 Len=1368 TSval=349269 TSecr=3017774295
745 249.579025   192.168.137.37            googleapis.l.google…    TLSv1.2   397 Application Data
```

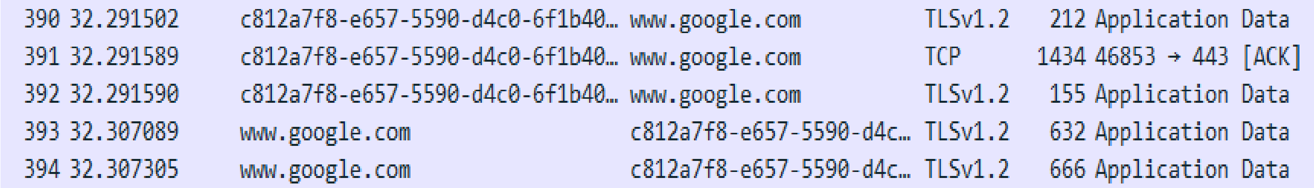
그림 2 모바일 기기(앱)과 구글 홈 미니 클라우드 서비스 사이의 네트워크 트래픽 캡쳐.
Fig. 2. Network traffic collection between the mobile device (app) and the Google Home Mini cloud service.

Figure 2 shows the network packet between the mobile and the cloud. During this time, the commands have been given to the Google Home mobile application. As Figure 3 shows, Google APIs and mobile share the application data with TLSv1.2, which is encrypted. Also, sometimes use the latest encryption protocol TLSv1.3 encryption as well [1].



```
11.566700    192.168.137.37                 googleapis.l.google.com TLSv1.3   583 Client Hello
11.728772    googleapis.l.google.com        192.168.137.37          TLSv1.3  2954 Server Hello, Change Cipher Spec
11.734361    googleapis.l.google.com        192.168.137.37          TLSv1.3  2288 Application Data
11.746815    192.168.137.37                 ytimg-edge-static.l.go… TLSv1.3   583 Client Hello
11.839652    192.168.137.37                 googleapis.l.google.com TLSv1.3   130 Change Cipher Spec, Application Data
11.912633    ytimg-edge-static.l.google.com 192.168.137.37          TLSv1.3  2954 Server Hello, Change Cipher Spec
11.920851    ytimg-edge-static.l.google.com 192.168.137.37          TLSv1.3   572 Application Data
11.924652    192.168.137.37                 ytimg-edge-static.l.go… TLSv1.3   130 Change Cipher Spec, Application Data
11.985559    googleapis.l.google.com        192.168.137.37          TLSv1.3  1122 Application Data
```

그림 3 TLSv1.3을 이용한 모바일 기기(앱)과 구글 홈 미니 클라우드 서비스 사이의 네트워크 트래픽 캡쳐.
Fig. 3. Network traffic collection between the mobile device (app) and the Google Home Mini cloud service using TLSv1.3.



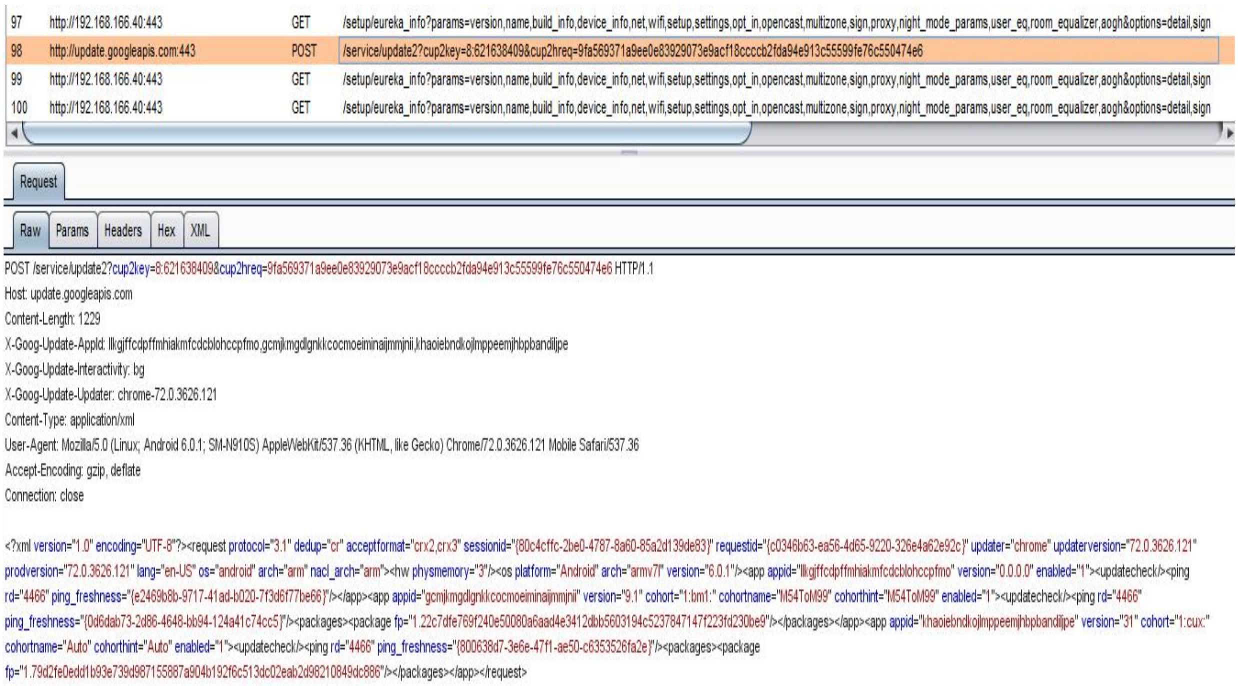
```
390 32.291502   c812a7f8-e657-5590-d4c0-6f1b40… www.google.com           TLSv1.2    212 Application Data
391 32.291589   c812a7f8-e657-5590-d4c0-6f1b40… www.google.com           TCP       1434 46853 → 443 [ACK]
392 32.291590   c812a7f8-e657-5590-d4c0-6f1b40… www.google.com           TLSv1.2    155 Application Data
393 32.307089   www.google.com                  c812a7f8-e657-5590-d4c… TLSv1.2    632 Application Data
394 32.307305   www.google.com                  c812a7f8-e657-5590-d4c… TLSv1.2    666 Application Data
```

그림 4 구글 홈 미니 스피커(기기)와 구글 홈 미니 클라우드 서비스 사이의 네트워크 트래픽 캡쳐.
Fig. 4. Network traffic collection between the Google Home Mini speaker (device) and the Google cloud service.

Figure 4 is the network packet between the Google Home Mini and google browser. It is captured when the command has given to the device. As Figure 4 shows, it also uses the TLSv1.2 encryption to share the application data.

After finding encrypted network traffic using Wireshark, we used Zenmap to discover the open ports as a first step to detect any vulnerabilities. The test takes the same setup condition as Wireshark. There were five open ports for the Google Home Mini in TCP protocol, and it is also the same for UDP protocol. In the previous research [14] also showed same number of the ports so it seemed to be fixed open ports. Among these ports, the test focuses on two ports, which are 8009 and 8443. We used Telnet to test open ports for listening status and service detection. Through Telnet testing, all five ports were found to be listening. Then, we investigated those ports with Kali Linux. For the test, without using hotspot of the laptop, put speaker, mobile phone and laptop in the same network, which is neo_house6.

Basic known attacks were conducted against the open ports using Metasploit. No ports were immediately vulnerable to known attacks. Next, we moved to a local API test.



```
97   http://192.168.166.40:443         GET   /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,opencast,multizone,sign,proxy,night_mode_params,user_eq,room_equalizer,aogh&options=detail,sign
98   http://update.googleapis.com:443  POST  /service/update2?cup2key=8:621638409&cup2hreq=9fa569371a9ee0e83929073e9acf18ccccb2fda94e913c55599fe76c550474e6
99   http://192.168.166.40:443         GET   /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,opencast,multizone,sign,proxy,night_mode_params,user_eq,room_equalizer,aogh&options=detail,sign
100  http://192.168.166.40:443         GET   /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,opencast,multizone,sign,proxy,night_mode_params,user_eq,room_equalizer,aogh&options=detail,sign
```

```
POST /service/update2?cup2key=8:621638409&cup2hreq=9fa569371a9ee0e83929073e9acf18ccccb2fda94e913c55599fe76c550474e6 HTTP/1.1
Host: update.googleapis.com
Content-Length: 1229
X-Goog-Update-AppId: llkgjffcdpffmhiakmfcdcblohccpfmo,gcmjkmgdlgnkkcocmoeiminaijmmjnii,khaoiebndkojlmppeemjhbpbandiljpe
X-Goog-Update-Interactivity: bg
X-Goog-Update-Updater: chrome-72.0.3626.121
Content-Type: application/xml
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; SM-N910S) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Mobile Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close

<?xml version="1.0" encoding="UTF-8"?><request protocol="3.1" dedup="cr" acceptformat="crx2,crx3" sessionid="{80c4cffc-2be0-4787-8a60-85a2d139de83}" requestid="{c0346b63-ea56-4d65-9220-326e4a62e92c}" updater="chrome" updaterversion="72.0.3626.121"
prodversion="72.0.3626.121" lang="en-US" os="android" arch="arm" nacl_arch="arm"><hw physmemory="3"/><os platform="Android" arch="armv7l" version="6.0.1"/><app appid="llkgjffcdpffmhiakmfcdcblohccpfmo" version="0.0.0.0" enabled="1"><updatecheck/><ping
rd="4466" ping_freshness="{e2469b8b-9717-41ad-b020-7f3d6f77be66}"/></app><app appid="gcmjkmgdlgnkkcocmoeiminaijmmjnii" version="9.1" cohort="1:bm1:" cohortname="M54ToM99" cohorthint="M54ToM99" enabled="1"><updatecheck/><ping rd="4466"
ping_freshness="{0d6dab73-2d86-4648-bb94-124a41c74cc5}"/><packages><package fp="1.22c7dfe769f240e50080a6aad4e3412dbb5603194c5237847147f223fd230be9"/></packages></app><app appid="khaoiebndkojlmppeemjhbpbandiljpe" version="31" cohort="1:cux:"
cohortname="Auto" cohorthint="Auto" enabled="1"><updatecheck/><ping rd="4466" ping_freshness="{800638d7-3e6e-47f1-ae50-c6353526fa2e}"/><packages><package
fp="1.79d2fe0edd1b93e739d987155887a904b192f6c513dc02eab2d98210849dc886"/></packages></app></request>
```

그림 5 Burp Suite를 이용하여 발견된 몇가지 APIs
Fig 5. Some of APIs are found by using Burp Suite

By using Burp Suite, some APIs are found which are the app_device_id and parameters for version, name, build_info, device_info, net, wifi, setup, settings, opt_in, opencast, multizone, sign, proxy, night_mode_params, user_eq, room_equalizer, aogh&options in figure 5. Also, aglio [5] has created an unofficial APIs that is used between the Google Home app and Google Home so apply some APIs to the Google Home Mini to find the APIs. Findings are in Table 2.

표 3 구글 홈 미니 로컬 네트워크로부터 반환된 API 호출과 정보 값
Table 2. API calls and information returned from a Google Home Mini on the local network.

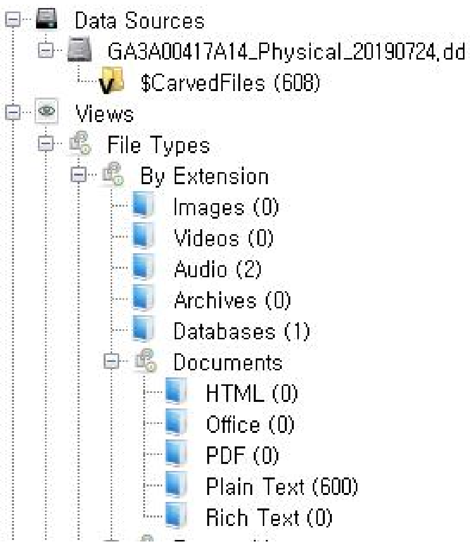
Type	Info	API	Returned
GET	Parameters	http://192.168.166.40:8008/setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,opencast,multizone,sign,proxy,night_mode_params,user_eq,room_equalizer,aogh&options=detail,sign	device_info: cloud_device_id: ″D2C293358C936F11757914443A7C3F57″, factory_country_code: ″US″, hotspot_bssid: ″FA:8F:CA:98:A5:5B″, mac_address: ″20:DF:B9:4E:87:FE″, manufacturer: ″Google Inc.″, model_name: ″Google Home Mini″, product_name: ″mushroom″, name: ″Office speaker″, net: ip_address: ″192.168.166.40″, settings: country_code: ″KR″, locale: ″en-US″, timezone: ″Asia/Seoul″, wifi: bssid: ″90:9f:33:db:10:de″, ssid: ″neo_house6″
GET	Eureka Info	http://192.168.166.40:8008/setup/eureka_info	bssid: ″90:9f:33:db:10:de″, hotspot_bssid: ″FA:8F:CA:98:A5:5B″, ip_address: ″192.168.166.40″, locale: ″en-US″, location: country_code: ″KR″, latitude: 255, longitude: 255 mac_address: ″20:DF:B9:4E:87:FE″, name: ″Living Room″, ssid: ″neo_house6″,

			timezone: ″Asia/Seoul″, uma_client_id: ″cc918aa3-2bba-46d2-aa3c-bfe1fa3c275b″
GET	offer	http://192.168.166.40:8008/setup/offer	token: ″ADtqmfTJx82eFvi_wg3BOUfBcUmZgF_ik7veTnYR0hc9MTyJxXQZIJb_OY4B2CEvZizrabJqcZp4DyjvCPBV53Ya1qJ05SdNiY5zxADnaIB04sSiflT-IjZUj2yaowZFQxlQUFHLiKDm″
GET	Time zone	http://192.168.166.40:8008/setup/supported_timezones	display_string: ″Hawaii-Aleutian Standard Time (Honolulu)″, timezone: ″Pacific/Honolulu″ display_string: ″Hawaii-Aleutian Daylight *support many different time zone
GET	Supported locales	http://192.168.166.40:8008/setup/supported_locales	display_string: ″Amharic - አማርኛ″, locale: ″am″ display_string: ″Arabic - العربية″, locale: ″ar″ *support many different locales
GET	Alarm	http://192.168.166.40:8008/setup/assistant/alarms	day: 1, month: 4, year: 2019 fire_time: 1554108270000, id: ″alarm/5d762a93-0000-20b9-9fa8-f4f5e80b89c8″, status: 1, time_pattern: hour: 17, minute: 44, second: 30
GET	Bluetooth	http://192.168.166.40:8008/setup/bluetooth/status	connected_devices: device_class: 5898764, mac_address: ″10:92:66:13:c0:4a″, name: ″Hallym Simon (Galaxy Note4)″
GET	Configured network	http://192.168.166.40:8008/setup/configured_networks	ssid: ″me″, ssid: ″DESKTOP-ENIL7DS 3926″, ssid: ″neo_house6″
POST	App device ID	http://192.168.166.40:8008/setup/get_app_device_id	″app_device_id″: ″D2C293358C936F11757914443A7C3F57″
POST	Internet download speed	http://192.168.166.40:8008/setup/test_internet_download_speed	″bytes_received″: 31457280, ″response_code″: 200, ″time_for_data_fetch″: 21807, ″time_for_http_response″: 819
POST	Scan Wi-Fi	http://192.168.166.40:8008/setup/scan_wifi	Response 200
GET	Scan results	http://192.168.166.40:8008/setup/scan_results	bssid: ″90:9f:33:db:10:de″, bssid: ″90:9f:33:db:10:de″, ssid: ″neo_house6″

The data can be used for investigation. For example, tokens can be a key to extract the data from the cloud. In parameters and some APIs have the network information of the speaker, which can tell which network the speaker is using. Other AI products connected through this network can also be identified. If the Bluetooth function is on, the investigator can check the information of the device connected to the speaker. If the speaker is connected to the mobile, it can discover the user's mobile model and MAC address.

5. Chip-off Analysis

After imaging the chip off data, a small file of 90,213KB was created and it was all in carved files. The carved files are analyzed with Autopsy 4.10.0.



Data Sources
GA3A00417A14_Physical_20190724.dd
$CarvedFiles (608)
Views
File Types
By Extension
Images (0)
Videos (0)
Audio (2)
Archives (0)
Databases (1)
Documents
HTML (0)
Office (0)
PDF (0)
Plain Text (600)
Rich Text (0)

그림 6 Autopsy로 오픈한 .dd 파일
Fig. 6..dd file opened with Autopsy to analyze

Bunch of log text files are stored but it does not contain much information. Table 3 shows some findings.

표 4 칩오프로 추출된 로그 텍스트
Table 3. Acquired log text data from chip-off

File name	Data
F0161412	RAM: 476992K total, 271004K free, 42636K buffers, 83604K cached, 108K shmem, 9252K slab Kernel log
F0166284	NAND device: Manufacturer ID: 0x98, Chip ID: 0xda (Toshiba 256MiB 8-bit)
F0168388	Product name: mushroom Product model: Google Home Mini Wifi.interface: mlan0 Wifi.ap.dev_name: ipTIMEAP Wifi.ap.manufacturer: ipTIME Wifi.ap.model.name: ipTIMEAP Wifi.ap.modle_number: 1234567890 Wifi.ap.vendor_prefix: [90:9f:33]
F0167416	OS platform: Linux
F160746	User name: Hallym simon Phone model: Galaxy Note 4 MAC address: [10:92:66:13:c0:4a]

The .ogg files were open with Groove 2018 from Microsoft and VLC media player (version 3.0.7.1) but all failed. Even converted ogg to mp3 file, did not work. In addition, the sqlite file was also not able to open. It is expected that corruption would have occurred during the imaging process.

Ⅴ. Conclusion

Through the test, several facts are confirmed. First, Google Home Mini does not store much data in the app. Second, by using Wireshark, it has found that how Google Home Mini, Google Home app and the Google cloud exchange data. They exchange the data using TLSv1.2 encryption and occasionally using the latest version of encryption TLSv1.3. Third, Google Home Mini has five open ports, which are HTTP, ajp13, https-alt, cslistener and scp-config. The vulnerability tests on the ajp13 and https-alt ports are done, and they are not exploitable. Then use the Burp suite and

Postman to find the local APIs. In the API, some essential data exists, like tokens that can be used for cloud data, configured network information of speakers, Wi-Fi information, setting country for speaker, time zone, and Bluetooth information. For chip off, not much data is stored These data can be applied if the suspect has a Google Home Mini in his house, and the suspect is denied telling its use and connection between them. Additional work still needs to be done on the device, application and network levels of the Google home mini to find additional, potentially hidden, data. Further, software updates for the GHM are frequent, and new artefacts may be introduced with each new update. Also, this test has don only for Android. Thus, the test for iOS will be needed to get more date about Google Home devices.

Acknowledgments. This work is funded by the KIAT (Korea Institute for Advancement of Technology) grant number N0002260. Thank you to Hancom GMD for support on the project.

참고문헌 (Reference)

〔1〕 An Overview of TLS 1.3 – Faster and More Secure 〔WWW Document〕, 2016. . Kinsta Managed WordPress Hosting. URL https://kinsta.com/blog/tls-1-3/ (accessed 4.2.19).

〔2〕 Chung, H., Park, J., Lee, S., 2017. Digital forensic approaches for Amazon Alexa ecosystem. Digital Investigation 22, S15–S25. DOI: https://doi.org/10.1016/j.diin.2017.06.010

〔3〕 Dipert, B., n.d. Teardown: Google's Home Mini 〔WWW Document〕. EDN. URL https://www.edn.com/design/consumer/4460586/2/Teardown—Google-s-Home-Mini (accessed 4.1.19).

〔4〕 Gibbs, S., 2017. Google Home Mini review: a brilliant little £50 voice assistant speaker. The Guardian.

〔5〕 Google Home 〔WWW Document〕, n.d. URL https://rithvikvibhu.github.io/GHLocalApi/#top (accessed 5.20.19).

〔6〕 Google's Home Mini outsmarts but doesn't outperform Amazon's Echo Dot 〔WWW Document〕, 2019. Digital Trends.
URL https://www.digitaltrends.com/smart-home-reviews/google-home-mini-review/ (accessed 5.7.19).

〔7〕 OK Google is More Than OK for Digital Forensics Investigations, 2018. . Cellebrite. URL https://www.cellebrite.com/en/blog/ok-google-is-more-than-ok-for-digital-forensics-investigations/ (accessed 3.31.19).

〔8〕 Technical Specs for Google Home Mini – Google Store 〔WWW Document〕, n.d. URL https://store.google.com/gb/product/google_home_mini_specs (accessed 4.1.19).

〔9〕 Which SSL/TLS Protocol Versions and Cipher Suites Should I Use? 〔WWW Document〕, 2015. . Independent Security Evaluators. URL https://www.securityevaluators.com/ssl-tls-protocol-versions-cipher-suites-use/ (accessed 5.7.19).

〔10〕 Wohlwend, W.H.M.S.M.W.J., 2017. Security Analysis of the Amazon Echo.

〔11〕 The picture of google home mini tear down〔WWW Document〕, 2019. . giggle hardware. URL https://gigglehd.com/gg/lifetech/4174947 (accessed 5.7.19).

〔12〕 Clinton, I., Cook, L. and Banik, S., 2016. A Survey of Various Methods for Analyzing the Amazon Echo.

〔13〕 Hyde, J. and Moran, B., 2017. Alexa, are you Skynet. SANS Digital Forensics and Incident Response Summit.

〔14〕 Investigating Rebel Scum's Google Home Data – SANS DFIR Summit 2018 – YouTube 〔WWW Document〕, n.d. URL https://www.youtube.com/watch?reload=9&v=dLQLJP0Cu7c (accessed 8.7.19).

저자소개

박 민 진 (Min Jin Park)

Min Jin Park is a Master's course Student in the Legal Informatics and Forensic Science Institute at Hallym University. Her research interests include digital forensic investigation , IoT Forensic, Security.

제임스 조슈아 (Joshua Isaac James)
정회원
Joshua I. James is a Professor in the Legal Informatics and Forensic Science Institute at Hallym University. His research focus area is advanced automation in digital forensic investigations.