D. Ferraris, D. Bastos, C. Fernandez-Gago, F. El-Moussa, and J. Lopez, "An Analysis of Trust in Smart Home Devices", *The 20th World Conference on Information Security Applications: WISA-Workshop 2019*, In Press.
NICS Lab. Publications: https://www.nics.uma.es/publications

An Analysis of Trust in Smart Home Devices

Davide Ferraris[1], Daniel Bastos[2], Carmen Fernandez-Gago[1], Fadi El-Moussa[2], and Javier Lopez[1]

[1] Network, Information and Computer Security Lab, University of Malaga, 29071 Malaga, Spain
{ferraris,mcgago,jlm}@lcc.uma.es
[2] British Telecom, Adastral Park, Ipswich, IP5 3RE, United Kingdom
{daniel.bastos,fadiali.el-moussa}@bt.com

Abstract. In recent times, smart home devices like Amazon Echo and Google Home have reached mainstream popularity. These devices are intrinsically intrusive, being able to access user's personal information. There are growing concerns about indiscriminate data collection and invasion of user privacy in smart home devices. Improper trust assumptions and security controls can lead to unauthorized access of the devices, which can have severe consequences (i.e. safety risks). In this paper, we analysed the behaviour of smart home devices with respect to trust relationships. We set up a smart home environment to evaluate how trust is built and managed. Then, we performed a number of interaction tests with different types of users (i.e. owner, guests). As a result, we were able to assess the effectiveness of the provided security controls and identify some relevant security issues. To address them, we defined a trust model and proposed a solution based on it for securing smart home devices.

Keywords. Internet of Things (IoT), Trust, Security, Smart Home.

1 Introduction

The global smart home market is expected to reach US$ 113 billion by 2022, more specifically, smart speakers are experiencing massive market growth, with shipments growing 187% in the second quarter of 2018[3]. There are two main competitors in this market: Amazon and Google. They have both released smart speakers: Amazon Echo devices and Google Home devices. These devices include their own voice assistants, Alexa[4] and Google Assistant[5], which have capabilities like setting up calendar appointments, ordering food, playing music or creating shopping lists. The smart speakers are also able to connect to other IoT devices in the smart home environment, allowing users to control multiple devices only by voice. A direct consequence of the number of functionalities offered by these smart speakers is an implication of trust by the user. The concept of trust is

[3] https://www.canalys.com/
[4] https://www.alexa.com/
[5] https://store.google.com/es/product/google_home_mini

difficult to define because it is strongly dependent on the context and it can be related to many different topics [3]. However, in the majority of cases, the users' trust in a product is an enabler of its success [9]. For this reason, we argue that there is the need to further understand and improve how smart home devices interact and build trust among IoT devices, especially smart speakers.

The structure of the paper is as follows. In Section 2 we describe the related work. Then, in Section 3 we set up the smart home scenario and in Section 4 we perform the trust analysis. Our proposed trust-based solution is described in Section 5. Finally, in Section 6 we show the conclusions.

2 Related Work

According to Moyano et al. [7], we refer to trust as "the personal, unique and temporal expectation that a trustor places on a trustee regarding the outcome of an interaction between them". By this definition, we have to consider two actors: a trustor and a trustee. The trustor is the actor needing the trustee to fulfil an action. Trust is fundamental to help the trustor decide which trustee to consider in order to start the interaction and to accept its outcome. Trust is strongly related to security in Information Technology [6, 9] and also in the field of IoT [5]. The IoT allows smart devices to be used through the Internet anywhere and anyhow [11]. These devices need to be secured through the Internet and they need to trust the other devices in order to interact with them [13] often through protocols that raise security risks [1]. How trust is built depends strongly on the type of IoT architecture [4] where smart speakers such as Amazon Alexa Echo Dot and Google Home Mini are becoming very popular. In [10], the authors studied the growing interaction between humans and smart speakers. However, there is currently only a few research works on trust and security regarding the relationship among smart home devices, voice assistants and the end users. In [2] the authors investigated how Intelligent Virtual Assistants (IVA) are now used and how trust could be considered according to the security and privacy of the users. Although, this work is just to let the customers aware of the dangers related to IVA devices. Considering other smart home devices, Notra et al. [8] proposed a solution to protect devices such as Philips Hue Lights by restricting access at the network level. They stated that it is hard to standardize a security implementation into IoT devices due to the heterogeneity of vendors, so they proposed a cloud service to guarantee Security as a Service. Although, trust is not considered and security issues are still present in the cloud component. Finally, up to now, there is no work related to the Google Home Mini.

In our work, we investigate how the IVA communicate with the Philips Hue Lights, the smartphone apps and the cloud. We focus on how the IVA build their trust in the user and how their trust models can be improved.

3 Smart Home Scenario: Set-Up

We developed an experiment which mimics a smart home scenario to analyse the processes used by Google Home Mini (GH), Amazon Echo Dot (AE) and

Philips Hue Lights (PHL) to establish and maintain trust among themselves and the users.

Users and Devices. In our experiment, we considered the following users: the owner of the house (HO), a member living in the house (HM), a house guest (HG) and a malicious user (MU). We consider HO as a fully trusted user, HM as somewhat trusted and the HG and MU as untrusted. Each user owns a smartphone but only HO and HM have access to the home Wi-Fi network. The devices used in the experiment are: one modem, one Desktop Computer, three Android smartphones, one AE, one GH and one PHL Starter Kit.

Set-up and Connection to Wi-Fi The experiment started with the creation of a dedicated Wireless Access Point (WAP) in the Desktop computer, where we also configured a network sniffer in order to get a deeper look on how the devices communicate. We connected the HO smartphone to the newly created WAP and installed the Alexa[6] and Google Home apps[7]. Both apps require the user to register an account. When they are switched on for the first time, both AE and GH create their own WAP, hereafter called Google WAP (GWAP) and Amazon WAP (AWAP). Then, using the respective apps, the HO was able to connect to the devices and configure their access to the home Wi-Fi network. We discuss later which issues are raised in this phase. After the pairing process was completed, both the GWAP and AWAP disappeared. On the contrary, in order to set up the PHL, we needed to connect the included hub called Hue Bridge that communicates with the smart lights using a radio protocol called Zigbee[8]. Wi-Fi connection is not available on the Hue Bridge. Therefore, we connected it by Ethernet cable to the desktop computer. Then, we installed the Philips Hue app[9] in both the smartphones of HO and HM, creating Philips Hue accounts for each of them. We configured the HO smartphone to find and control the lights, which required pressing a button directly on the Hue Bridge to pair the devices. The PHL can be controlled using the Hue app or, after configuration, by the AE or the GH (both by voice or apps). To configure the PHL with the AE, we had to install the Philips Hue Alexa Skill, which is an official plugin, using the Alexa app, allowing the HO's smartphone to be able to connect and control the lights. For the configuration with the GH, we had to use the trusted devices list available inside the Home app on the HO's smartphone to add the PHL in order to connect and control it. Finally, for the HG smartphone, we downloaded the Alexa, Home and Hue apps and created individual accounts for each of them using the cellular network connection.

Interaction Tests and Access/Control. We chose to perform tests based on two factors: popularity[10] and practical implications. Considering voice interactions, we asked the devices news update, check the HO calendar, to set up an alarm, to play a song, to increase/decrease the volume, to turn on/off the

[6] https://play.google.com/store/apps/details?id=com.amazon.dee.app
[7] https://play.google.com/store/apps/details?id=com.google.android.apps.chromecast.app
[8] https://www.zigbee.org/
[9] https://play.google.com/store/apps/details?id=com.philips.lighting.hue2
[10] //www.which.co.uk/reviews/smart-home-hubs/article/smart-hubs-explained/google-assistant-and-alexa-commands

lights. These commands can raise privacy implications (i.e. news update, check calendar appointment) or affect the external environment (i.e. sound, lights). Regarding app interactions, we used Alexa and Home apps to check/control current activities (i.e. music cast), to increase/decrease the volume, check historical events and HO info. Moreover, we used Alexa, Home and Hue apps to turn on/off lights. Also in this case, we consider commands that can raise privacy implications (i.e. check historical events and HO info) or affect the environment (i.e. switching on/off the lights). We looked at the available methods for the HO to share access/control of each IoT device, considering HM and HG as examples. We discuss this possibility in the following section. Finally, while analysing the traffic, we were able to read communications in clear. For example, if the user asked to reproduce the news, it was possible to see the destination address of the requested services (i.e. BBC news). A possible way to address this issue could be to use a single service for every request, so it would be impossible to recognize which network data was related to which actions.

4 Smart Home Devices: Trust Analysis

We found similarities on how AE, GH and PHL work, although some key differences are present. **Amazon Echo Dot (AE)** When the device is powered on for the first time, it creates its AWAP and trusts anyone with an Alexa app to start configuring the device. This is necessary to enable a user to pair the device. Anyone within the AWAP range will be able to notice that there is a new AE device available for configuration. This means all the users in our experiment, including the MU, are able to configure and take ownership of the device during this stage. This is the only weak point of the AE configuration process. After the AE is configured to a home Wi-Fi network its own AWAP disappears. In the event the home Wi-Fi network becomes unavailable, only the paired user will be able to configure the Wi-Fi network and control AE through its app. The Alexa app is designed to work as a standalone app, so it asked for many permissions from the Android test smartphones (i.e. Contacts, Camera, Location, Microphone). From a trust perspective, it requires the user to trust the app with access personal data stored in the smartphone. The AE supports voice recognition, but this feature is not enabled by default. Consequently, all the users are able to perform voice interactions and for AE they are all the same user. Hence, configuring voice recognition is highly desirable in order to prevent anyone from check calendar appointments or controlling sound and lights. Conversely, the Alexa app restricts access to the AE only to the HO. This means that the information about the device, its owner or the data history is also only available to the HO. **Google Home Mini (GH)** Similarly to the AE, the GH created its own GWAP when powered on for the first time, allowed anyone to connect and configure it using the Home app, and the GWAP disappeared if configuration was successful. However, whenever there was no known Wi-Fi network around, the WAP reappeared. This happened because the GH only records the last configured Wi-Fi network details, posing a security problem since every user

is trusted at this point. The HG was able to re-configure the device to a different Wi-Fi network. After this point, the legitimate users were not able to control the device anymore using the Home app neither to control the other smart devices connected to the GH (because they are still connected to HO's Wi-Fi network). The only way for the HO to take again control of the device was to hard reset it. As for the Home app, it is designed to work in the presence of GH devices, as opposed to the Alexa app which can work as standalone, so it asked fewer permissions from our test Android smartphones (only Contacts and Location). The Home app restricted access to the GH to all the users on the same Wi-Fi network (HO and HM), so the HM is considered trusted. However, he must pair his device with GH first. Then, the range of activities that the HM is allowed to perform is broad: he/she is able to see the current activity, play, pause and stop songs, control the sound volume, see the name of the owner of the device and even change the name of the device. However, access to the lights is restricted only to the HO. Nonetheless, the range of activities allowed to the HM can be considered a trust violation since the HO has no control over it. Even if HO wants to disable this kind of access, it is impossible to do it. The HG, having no access to the Wi-Fi network, was not able to access or perform any activities on the GH using the app. In the event of the HM turning malicious or the HG somehow getting access to the Wi-Fi credentials, there are a number of negative consequences we can identify. For example, if the HO sets up a morning alarm the HM or HG could restrict/disable that alarm just by lowering the sound level to zero. The HM and HG could also access the HO calendar and make changes. Regarding voice interactions, all users could interact with the device as if they were the HO. The GH also supports voice recognition but it is not mandatory to configure it by default. Once again, making voice recognition mandatory for the HO would help solve this issue.

Philips Hue Lights (PHL) Configuration of the PHL is achieved by pairing the Hue Bridge with a smartphone using the Hue app. The Hue Bridge and the smartphone need to be connected to the same network, which means the HG is not able to configure the Hue lights or connect to the Hue Bridge. The pairing process required physical access to the Hue Bridge pushing a button on the same Hue Bridge during the configuration. From a trust perspective, this is a good security measure since it requires the user to be next to the device. This set-up procedure is the most trust-oriented one from all the tested devices.

However, while sniffing traffic we noticed that the smartphone communicated with the Hue Bridge using an insecure REST API (http clear text). PHL also used SSDP (Simple Service Discovery Protocol) to announce itself in the network, revealing its Bridge ID, IP location, serial number of the device, model name, model number and other details in clear text. This means sensitive details were visible for someone in the same network (e.g. the HM), allowing for reverse engineering of authentication details and subsequent control of the device. Moreover, it was possible to discover if a user is switching on or off the lights when using Alexa voice commands since the information is transferred in clear text (code {"on":true} and code {"on":false}). However, when using the apps to perform the same task, the information was encrypted. The HO can

share access to the lights by providing an email address of a Hue account user within the Hue app. Control of the lights can also be shared using the Home and Alexa apps after they are paired with the Hue bridge if HO shared complete control with HM. This method bypassed the creation of a Hue account for the user who is receiving access, somehow breaking the trust controls of the Philips Hue lights. Voice commands in order to control the lights (e.g. turn on/off and change intensity) were also possible by any user when voice recognition was not configured. However, using custom names for the lights can be a measure to help prevent unauthorized interactions.

5 Proposed Trust Model

The set-up phase shows a limitation for both AE and GH devices, in fact, through the initial AWAP and GWAP, every user was able to take ownership of the device. To be sure that a user is trusted, we suggest the PHL approach pushing a button on the device. In addition, this issue remains for GH each time the GWAP appears. This is a severe security issue. However, we can revert this by using the same approach used by AE (allowing only the HO to configure the device). For the AE and PHL, through their apps, the only trusted user is the HO. This implementation can be considered a limitation because other legitimate users are not able to control or check the devices using their apps. On the other hand, the GH allows the HM to control or check the device.

Thus, to improve all the models related to GH, PHL and AE, we suggest implementing a new trust model. This model is composed of a score and a context value for each user. The owner has the ability to remove or limit the actions that another user can perform giving to them a score value according to a particular context of the actions. These parameters are presented in our trust model by implementing a simple trust metric for each user.

The trust metric is used to define rules for each user and it is represented by the following function:

$$Trust\_Metric_x : TM(R, C, S)$$

where the function $Trust\_Metric_x \in \Re$ and its parameters are:

1. Role (R). They have been presented earlier: HO, HM, HG and MU.
2. Context (C). It is the context related to the device or functionalities. It is represented by a number given by the HO. The higher the context, the higher the score or role needed. This value belongs to the following set: C {1,2,3,4}. The lower the value, the less important is C.
3. Score (S). It is the rank given to the users by the HO. It is similar to a reputation value. The more trusted the user is, the higher the score given. It belongs to the following set: S {0,1,2,3,4,5}.

In regards to the roles, the HO is allowed full access regardless of S and C, given that he/she is fully trusted. For a MU, the metric works in the opposite way, since he/she is not allowed to control or check anything. Even for this role,

C and S are optional. On the contrary, for the other roles (HM and HG) C and S are fundamental. The metric is very simple, so it is easily performed by any IoT device, even considering their limited computational power [12]. It computes a value that will be used to check which actions are allowed for a particular user and for a particular context. We propose three trust levels: high, medium and low. The high one allows the user to control the device. The medium level allows checking the devices' activity but denies control of the device. Finally, the low one means that the user is untrusted, so any connection is refused.

It is basically a subtraction of the value score respect to the value context. If the result is positive, the trust value is ranked as high. If the result is zero, the trust level is medium. Otherwise, the trust level is low. If a context has a value of 1, it means that it is not important for the owner (i.e. check the weather). On the other hand, if a context has a value of 4, it means that is very important (i.e. to do bank transactions). Therefore, we can say that if an HM has a value of 5, he or she is similar to an HO, considering that with this score value it is possible to control everything, whatever C is.

$$Trust\_Metric_1 : TM(HM, C, 5) > 0$$

Conversely, if a user has a score of 0, he or she is considered an MU and cannot perform actions for every C.

$$Trust\_Metric_2 : TM(MU, C, 0) < 0$$

We chose these values according to the explanation of the trust metric parameters given earlier. The score must have a bigger bound to include the role MU (score = 0) and the role HO (score = 5). For an MU, no matter the context, it must be impossible for him/her to perform actions. On the contrary, for an HO everything must be permitted. The values from 1 to 4 are used both for C and S to define the boundaries related to the other users (i.e. HM and HG). Using these roles we cover all the possible actors and for each of them, the scores could be different also for the same context.

6 Conclusion

In conclusion, our study reveals that security is being taken seriously by big name manufacturers but there is a lot of space for improvements in regards to how trust relationships are managed. The AE approaches security in a restrictive way, providing the owner of the device tight control over who interacts with it and not making many trust assumptions. On the other hand, the GH provides a more open approach by allowing any user on the same Wi-Fi network to interact with the device and cast media content. As a consequence, on the GH, a malicious user can potentially eavesdrop legitimate users or perform dangerous activities. To address these issues, we proposed a trust model that achieves a responsible balance between the openness of GH and the limitations of AE. Using this model, it is possible to create a trust score related to a user concerning a particular context. This model allows the owner of the home devices to have

more control on how the user interacts with them but still allows responsible sharing of the devices with other users.

Acknowledgement

This project has received funding from the European Union Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 675320 (NeCS). This work reflects only the authors' view and the Research Executive Agency is not responsible for any use that may be made of the information it contains.

References

1. Bastos, D., Shackleton, M., El-Moussa, F.: Internet of things: A survey of technologies and security risks in smart home and city environments. IET Conference Proceedings pp. 30 (7 pp.)–30 (7 pp.)(1) (January 2018)
2. Chung, H., Iorga, M., Voas, J., Lee, S.: Alexa, can i trust you? Computer 50(9), 100 (2017)
3. Erickson, J.: Trust metrics. In: Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on. pp. 93–97. IEEE (2009)
4. Ferraris, D., Daniel, J., Fernandez-Gago, C., Lopez, J.: A segregated architecture for a trust-based network of internet of things. In: 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (CCNC 2019). Las Vegas, USA (Jan 2019)
5. Ferraris, D., Fernandez-Gago, C., Lopez, J.: A trust-by-design framework for the internet of things. In: New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. pp. 1–4. IEEE (2018)
6. Hoffman, L.J., Lawson-Jenkins, K., Blum, J.: Trust beyond security: an expanded trust model. Communications of the ACM 49(7), 94–101 (2006)
7. Moyano, F., Fernandez-Gago, C., Lopez, J.: A conceptual framework for trust models. In: 9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2012. vol. 7449 of Lectures Notes in Computer Science, pp. 93–104. Springer Verlag (Sep 2012)
8. Notra, S., Siddiqi, M., Gharakheili, H.H., Sivaraman, V., Boreli, R.: An experimental study of security and privacy risks with emerging household appliances. In: Communications and Network Security (CNS), 2014 IEEE Conference on. pp. 79–84. IEEE (2014)
9. Pavlidis, M.: Designing for trust. In: CAiSE (Doctoral Consortium). pp. 3–14 (2011)
10. Purington, A., Taft, J.G., Sannon, S., Bazarova, N.N., Taylor, S.H.: Alexa is my new bff: social roles, user satisfaction, and personification of the amazon echo. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems. pp. 2853–2859. ACM (2017)
11. Roman, R., Najera, P., Lopez, J.: Securing the internet of things. Computer 44(9), 51–58 (2011)
12. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Computer Networks 57(10), 2266–2279 (2013)
13. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for internet of things. Journal of network and computer applications 42, 120–134 (2014)