D. Ferraris, D. Bastos, C. Fernandez-Gago, and F. El-Moussa, "A Trust Model for Popular Smart Home Devices", *International Journal of Information Security*, 2020.
http://doi.org/10.1007/s10207-020-00519-2
NICS Lab. Publications: https://www.nics.uma.es/publications

A Trust Model for Popular Smart Home Devices

Davide Ferraris[a], Daniel Bastos[b], Carmen Fernandez-Gago[a], Fadi El-Moussa[b]
[a]*NICS Lab*, *University of Malaga*, 29071 Malaga, Spain
{ferraris,mcgago}@lcc.uma.es
[b]*British Telecom,Orion Floor 5 pp10*, Adastral Park, Martlesham Heath, IP5 3RE, Ipswich, England
{daniel.bastos,fadiali.el-moussa}@bt.com

***Abstract*—Nowadays, smart home devices like Amazon Echo and Google Home have reached mainstream popularity. Being in the homes of users, these devices are intrinsically intrusive, being able to access details such as users' name, gender, home address, calendar appointments and others. There are growing concerns about indiscriminate data collection and invasion of user privacy in smart home devices, but studies show that perceived benefits are exceeding perceived risks when it comes to consumers. As a result, consumers are placing a lot of trust in these devices, sometimes without realizing it. Improper trust assumptions and security controls can lead to unauthorized access and control of the devices, which can result in serious consequences. In this paper, we explore the behaviour of devices such as Amazon Echo and Google Home in a smart home setting with respect to trust relationships and propose a trust model to improve these relationships among all the involved actors. We have evaluated how trust was built and managed from the initial set up phase to the normal operation phase, during which 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 potential relevant security issues. In order to address the identified issues, we defined a trust model and propose a solution based on it for further securing smart home systems.**

***Index Terms*—Internet of Things (IoT), Trust, Security, Privacy, Smart Home**

I. Introduction

Through the Internet of Things (IoT), each smart device can be addressable and cooperate through the Internet to fulfill a common objective [28]. Nowadays, after years of development, the IoT is a growing consumer technology. We can state that the capability of sensing and affecting the external environment is what classifies the IoT as a disruptive technology.

The global smart home market is expected to reach 113 billion US$ by 2022, making up for 33.4 billion US$ in 2017. More specifically, smart speakers are experiencing massive market growth, with shipments growing 187% in Q2 2018 [1]. There are two main competitors in this market: Amazon and Google. They have both released affordable smart speakers and although in 2017 the Amazon Echo line was the undisputed leader, in 2018 Google Home devices were taking over and leading in sales [2].

The included voice smart assistants, Alexa [3] and Google Assistant [4], feature capabilities like setting up calendar appointments, ordering food, playing music, creating shopping lists or answering to trivia questions. They are also able to communicate with other IoT devices in the smart home, allowing the users to control multiple devices using only voice commands. Other popular smart home devices include smart lights (i.e. Philips Hue) and security or baby cameras.

Due to the easy voice interactions and evolving list of features, smart speakers are becoming part of everyday life for many users [17, 32]. A research developed by Purington et al. [27] showed how the interaction between humans and Echo devices is growing. Moreover, a research developed by Wiederhold [35] shows how even children can be affected by these devices during their age development. Giesler and Fischer [12] analyzed how Echo devices are trusted by customers even if they do not work properly or behave in a strange way. An inevitable consequence of the amount of functionalities offered by the smart speakers is an implication of trust by the user. The concept of trust is difficult to define since trust is strongly dependent on the context and it can be related to many different topics [5]. For instance, we can refer to trust about the listening and comprehension capabilities of the smart assistants, trust on the actions that the device is going to take based on the commands, trust that the data collected by the device is kept safe or trust that there are no privacy violations [10]. Surveys have shown that a big share of users do not buy IoT devices because they do not trust them, but even if they buy them, they still do not trust that the data are collected and shared through the IoT in secure way [5] [6]. In any case, generally, the users' trust in a product is an enabler of its success [26]. This is true for software or hardware products and even more for IoT devices.

Trust is an important concept in IoT networks [6], as it can be used as an enabler to allow the IoT devices communicate among them. In this paper, we introduce a novel trust model that helps users and IoT devices (i.e. Alexa) to interact in a trusted way. In order to sustain it, we explore how IoT devices in a Smart Home communicate among them and with the external network, focusing on the interactions with the aforementioned voice assistants. Finally, we assess possible

[1]https://www.statista.com/page/compass
[2]https://www.canalys.com/
[3]https://www.alexa.com/
[4]https://store.google.com/es/product/google_home_mini
[5]https://mobileecosystemforum.com/programmes/analytics/iot-report-2016/
[6]https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1900060

security issues present in these devices and how our trust model could improve smart home security.

The structure of the paper is as follows. The motivation of the scenario is presented in Section II and the discussion about its trust perspective is performed in Section III. Then, our trust-based solution is presented in Section IV. In Section V, we describe the related work and why our trust model is needed compared to other works. Finally, in Section VI, we conclude and discuss the future work.

II. A Motivated Smart Home Scenario

Our aim with this work is to design a novel trust model to improve security and privacy in smart home environments. In order to develop it, we have investigated how current smart homes work, which threats are present [1] and how trust concepts can be used to mitigate them. Thus, we have developed an experiment, using real devices, to mimick a smart home scenario in order to analyse the processes used by IoT devices to establish and maintain trust among themselves and the users.

We have divided the process into the following phases: users and devices, set up and connection to Wi-Fi (account creation, app installation and configuration), device-to-device connections and configurations, interaction tests and access control sharing. The interaction tests were divided into voice interactions (Alexa and Google Assistant voice commands) and app interactions, to assess the behaviour of the devices.

In order to make the reading easier, we collect all the acronyms used in this paper in Table I.

TABLE I: Table of Acronyms

Amazon Echo Dot	AED
Amazon WAP	AWAP
Context	C
Context Importance	CI
Google Home Mini	GHM
Google WAP	GWAP
House Guest	HG
House or family Member	HM
House Owner	HO
Internet of Things	IoT
Intelligent Virtual Assistants	IVA
Malicious User	MU
Philips Hue Lights	PHL
Role	R
Score	S
Wireless Access Point	WAP

A. Users and Devices

We have considered the following users, representing different types of trusted or untrusted entities: the owner of the house (HO), a person also living in the house (HM), a house guest (HG) and a malicious user (MU).

1) **HO**. The HO is the owner of the house (i.e Alice). We assume that she is also the owner of the smart devices present in the smart home. As stated in [16], she can be considered the system administrator.
2) **HM**. We consider the possibility that the HO shares the smart home with others (i.e Bob, Charlie). Thus, a HM is living in the same house as the HO but he does not own the smart devices. The HM can be considered an authenticated user [25] that can access some functionalities of the smart devices.
3) **HG**. As stated by [16], a smart home is "expected to have guests" (i.e. Dave) and the HO "can not expect all of these people to be careful about security".
4) **MU**. A MU (i.e. Mallory) is an external user that wants to perform attacks to the smart home (i.e control the smart devices). According to the particularity of the smart devices, there are several attacks that can be performed [37]. We consider the possibility that a HG or a HM can turn into a MU.

We consider the HO as a fully trusted user, the HM as somewhat trusted (i.e. only trusted to perform a limited set of actions), and the HG and MU as untrusted. Each user has a smartphone and both the HO and HM have daily access to the Wi-Fi network, as opposed to HG that is required to be connected to the Wi-Fi only when he visits HO or HM. On the other hand, MU does not have Wi-Fi access. The devices used in the experiment are the following: one modem, one desktop computer, three Android smartphones, one Amazon Echo Dot (AED), one Google Home Mini (GHM) and one Philips Hue Lights (PHL) starter kit (with 3 light bulbs).

Figure 1 gives a detailed look of the experiment, highlighting the connections between devices and also the control flow among users and devices, and devices with other devices. We can see that the desktop computer connects to the modem and all the other devices connect to it through Wi-Fi for internet access, allowing it to see all the traffic. In addition, the HO with her smartphone has control of all the smart devices, while the HM does not have direct control even though his smartphone is connected to the Wi-Fi network.

TABLE II: Threat Model

User	Goal
HM	- Take ownership of the device - Perform forbidden actions
HG	- Access and control the IoT entities
MU	- Access the Wi-Fi network - Steal the control of smart devices - Control the data flow - Check the data flow

In Table II we can see the Threat model for each type of user. We do not consider the HO as a possible attacker because she is the owner of the devices and can perform any actions. HM can turn into malicious if he tries to take ownership of the devices or perform forbidden actions (i.e. to change the calendar of the HO). In addition, the HG can also turn into malicious if he tries to control or to access to the devices in order to perform actions that are not allowed to him. Finally, the MU can try to illegitimately access the Wi-Fi network, steal the control of the devices or to control/check the data flow of the devices. However, we assume that a recognized MU must have not physical access to the devices. This can be more difficult to achieve in the case a HM turns into MU.

Fig. 1: Connections and controls among users and devices

Anyhow, these threats are mitigated by the use of the trust model that we propose in Section IV-C.

B. 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 (i.e. Wireshark [7]) in order to obtain a deeper look on how devices communicate. Then, we connected the HO's smartphone to the newly created WAP and installed the Alexa [8] and Google Home apps [9] available on the Google Play Store [10]. Using the apps, we created as HO both an Amazon and a Google account. We did the same for the HM's smartphone. The configuration process to connect the Echo and Home devices to the WAP is similar. When they are switched on for the first time, both devices create their own WAP, hereafter called Google WAP (GWAP) and Amazon WAP (AWAP). Then, using their smartphone, the users are able to connect to the devices through their respective apps, subsequently configuring their access to the home Wi-Fi network. We discuss later which issues are raised in this phase by both devices.

After the pairing process was completed, both the GWAP and AWAP disappeared. On the contrary, in order to set up the PHL, it is required to connect the included hub called Hue Bridge that communicates with the smart lights using Zigbee [11]. Unfortunately, the Wi-Fi connection is not supported on the Hue Bridge. Therefore, we connected the Hue Bridge by an Ethernet cable to the desktop computer in order to make it reachable in the network. Then, we installed the Philips Hue app [12] in both the smartphones of HO and HM, creating each one a Philips Hue account. 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 the configuration, by the AED or the GHM (both by voice or apps). To configure the PHL with the AED, we had to install the Philips Hue Alexa skill. This is an official plugin, installed using the Alexa app, allowing the HO's smartphone to be able to connect and control the lights. For the configuration with the GHM, 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's smartphone, we downloaded the Alexa, Home and Hue apps and then created individual accounts for each of them using the cellular network connection. Figure 1 presents an overview of the experiment, highlighting the connections between devices and also the control flow among users and devices, and devices and other devices. It is shown that the desktop computer connects to the modem and all the other devices connect to it through

[7] https://www.wireshark.org/
[8] https://play.google.com/store/apps/details?id=com.amazon.dee.app&hl=it
[9] https://play.google.com/store/apps/details?id=com.google.android.apps.chromecast.app&hl=it
[10] https://play.google.com/store
[11] https://zigbeealliance.org/
[12] https://play.google.com/store/apps/details?id=com.philips.lighting.hue2

the Wi-Fi in order to obtain internet access. At this stage, the smartphone of the HO has control of all the IoT devices, while HM does not have direct control even though his smartphone is connected to the Wi-Fi network. HG is connected to the Wi-Fi but it must not be able to connect to the devices and MU does not have access either to the Wi-Fi network or the IoT devices.

C. Interaction Tests

With all the devices connected, the next step was to conduct tests. The following tests were performed both on AED and GHM using their respective voice assistants (Alexa and Google Assistant):

- Ask for news update.
- Ask to set up or check a calendar appointment.
- Ask to set up or disable an alarm.
- Ask to play or pause a song from Spotify[13].
- Ask to increase/decrease sound volume.
- Ask to turn on/off lights.
- Ask to change intensity/colour of lights.

In addition, these other tests were performed using the apps on the three Smartphones (Alexa, Home and Philips Hue app):

- Check/control current activity.
- Play or pause a song from Spotify.
- Increase/decrease sound volume.
- Turn on/off lights.
- Control intensity/colour of lights.
- Check historical events.
- Check device owner info.

These tests were chosen based on two factors: popularity[14] and pratical implications. In voice interactions, there is a popular and innocuous command (news update), one with privacy implications (check calendar appointment) and others that trigger actions that affect the external environment (sound and lights). In both applications, there are also commands related to sound and lights and a command with privacy implications (check historical events and HO info).

D. Access Control Sharing

IoT devices usually allow the HO to share access and control of the device with other users. Moreover, the HO might also have the option to remotely access and control the device from outside the home network (for PHL only). We looked at the methods available for the HO to share access and control of each IoT device with others, using the HM and the HG as examples. In addition, we looked at the method that each IoT device uses to allow the HO to access it remotely. In the next section, we will explain how the different devices enable access control.

[13]https://www.spotify.com

[14]//www.which.co.uk/reviews/smart-home-hubs/article/smart-hubs-explained/google-assistant-and-alexa-commands

III. Trust Perspective of the Smart Home Scenario

A. Users and Devices

All the tested IoT devices are tied to individual accounts, so the users need to set up these accounts in order to be able to use them. These accounts are the only form of authenticating the owner of the device. Therefore, for three different devices, three different accounts were required (Amazon, Google and Hue accounts). Considering the growing use of Smart Home devices, we envision a future where a user (i.e. HO) has ten or more accounts for devices in her house, which is definitely not ideal. A hijack of one of these accounts means that the attacker will be able to control the connected device. For this reason, the concept of trust can be helpful in order to create a general model enabling the devices to interact safely and securely with recognized trusted users and devices.

B. Set-up and Connection to Wi-Fi

During the different phases of the process, we found clear similarities on how the AED, the GHM and the PHL work, although some key differences are present.

1) Amazon Echo: When the device is powered on for the first time, the Echo creates a Wireless Access Point (AWAP) and trusts anyone with an Alexa app in order to start configuring the device. At this point, anyone within the Wi-Fi range will be able to notice that there is a new AED device available for configuration. An issue arises here due to the fact that all three smartphone users in our experiment, including the malicious one, are able to configure and pair themselves to the device during this stage. All of them, at this point, are equally trusted. This is a weak point of the AED configuration process. In fact, in this phase, AED trusts anyone within the AWAP range that has an Alexa app installed with an Amazon account.

After the AED is configured to a home Wi-Fi network, its own AWAP disappears. In the event that the home Wi-Fi network becomes unavailable, only the paired user will be able to configure the Wi-Fi network and control AED through its app. However, if the user (i.e. HO) unpaired herself from the device or if the device is restored to the factory data, then new users would be allowed to pair.

The device communicates using TCP (with TLS) and mDNS (for media casting purposes) protocols. An interesting detail we noticed was that while the AED uses the router defined DNS server during normal operation, if that DNS server stops replying for some reason (i.e. network failure) the AED tries to go around it and use the Google Public DNS servers (IP 8.8.8.8). This is a good approach to increase availability of the device's services.

2) Google Home: Similarly to the AED, the GHM creates its own GWAP when it is powered on for the first time and allows anyone to connect and configure it using the Google Home app. After the configuration, the GWAP disappears. However, whenever there is no known Wi-Fi network around (it only records the last Wi-Fi configured password), the GWAP appears again.

This approach is different with respect to the one taken by the AED presented earlier. At this point, every user is trusted, which is a potential security problem. In fact, every user is trusted at this point. So, even the MU is able to configure the device to a different Wi-Fi network. At this point, the legitimate users will not be able to control the device anymore using the Home app, neither to control the other smart devices connected to the GHM (because they are still connected to HO's Wi-Fi network). The only way for the HO to take again control of the device is to hard reset it, losing all historical data. The HO could also perform the same action if the MU Wi-Fi network becomes unavailable and take back the ownership of the device. Similarly to the AED, the GHM can be controlled by app or by voice.

The device uses a mix of protocols to communicate: TCP (with TLS), GQUIC (a lightweight protocol developed by Google) and mDNS (for media casting purposes). It also uses by default Google's Public DNS servers (IP 8.8.8.8) for DNS queries, which is something unusual. This can be seen as a protection mechanism against DNS attacks (i.e. DNS cache poisoning) but it can also be interpreted as a way for Google to have more control and visibility about what happens in the device.

One similarity between AED and GHM devices is that they both produce a high amount of traffic on the network, even when there is no interaction happening between the user and the device. The generated traffic is mostly comprised of encrypted communications with servers controlled by the respective companies (Amazon and Google), possibly containing device diagnostics. The servers are mostly located in USA, and considering we performed the experiment in a country inside the European Union (EU) this can be a topic of discussion regarding the GDPR compliance [34]. Another similarity is when the devices lose internet connectivity. They both enter a "panic mode" state in which they send a lot of packets with the intention to try to restore the internet connection. This can lead to network congestion and disrupt the normal operation of the WAP.

3) Philips Hue Lights: The configuration of the PHL is achieved by pairing the Hue Bridge with a smartphone using the Hue app. The process requires physical access to the Hue Bridge in order to press a button during configuration. The Hue bridge and the smartphone need to be connected to the same network (the Hue bridge connects through Ethernet cable and the smartphone through wireless), which means the guest is not able to configure the Hue lights. From a trust perspective, this is a good security measure since it requires the user to be physically next to the device. Actually, this set-up procedure is the most trust-oriented one from all the tested devices.

During the experiment, we noticed that the traffic between the Hue Bridge and the smartphone was not encrypted. This allowed us to read API calls to the Hue Bridge and its responses. After the authentication is performed, the Smartphone communicates with the Bridge using a REST API (http clear text) and exchanges information using JSON documents. Philips Hue uses SSDP (Simple Service Discovery Protocol) to announce itself in the network. It reveals its Bridge ID, IP location with xml (xml has serial number of the device, model name, model number, ip address, uuid), Linux kernel version, etc. This means the Bridge ID and other details like API calls are visible for someone in the same network (i.e. the person living in the house) who can sniff the traffic, allowing for reverse engineering of authentication details and subsequent control of the device.

C. Interaction Tests

1) Voice interactions: **Alexa** The AED supports voice recognition, but this feature is not enabled by default. In our case, all three users are able to perform all voice interactions and for the AED they are considered as the same user. About the cooperation with the lights, since access to the PHL was given to the AED, any user can now control the lights using voice commands. The only barrier is that the owner can define custom names for each light, which means other users have to guess the names that were given to the lights in order to be able to control them. Hence, configuring voice recognition is highly desirable in order to prevent anyone from changing alarms, check calendar appointments or controlling sound and lights.

As for the other tests, when we asked Alexa for the news update, the AED contacted BBC [15] by default and we noticed that the network traffic communication with BBC was performed using the Hypertext Transfer Protocol (http). The channel used by BBC for the news does not use encryption by default so it is possible to see all the information being transmitted when news update is asked. The information is shown in Figure 2.

Google Assistant Regarding voice interactions, the GHM also supports voice recognition but it does not force the HO to configure it by default. For all the other interactions tested, we obtained the same results as with AED. Once again, configuring voice recognition would solve this issue, giving access to perform the tasks only to the legitimate users. But without voice recognition, if the HO has given GHM access to her calendars, Gmail or other personal information, any user can ask the GHM device about that information. Given this was a design choice made by GHM [16], we believe it constitutes a potential privacy and security issue. Regarding the news update, Google Assistant contacts BBC if it is specified by the owner on the app. Otherwise, the device selects the most suitable stream according to the location. If BBC is used, then traffic can be seen as it is unencrypted (like for AED).

2) App interactions: **Alexa App** It is interesting to highlight that the Alexa app is designed to work as a standalone app, with or without any Amazon IoT devices around, so it asked multiple permissions from our test Android smartphones (i.e. contacts, camera, location, Memory, Microphone, SMS and

[15]https://www.bbc.com/

[16]https://support.google.com/googlenest/answer/7177221?hl=en

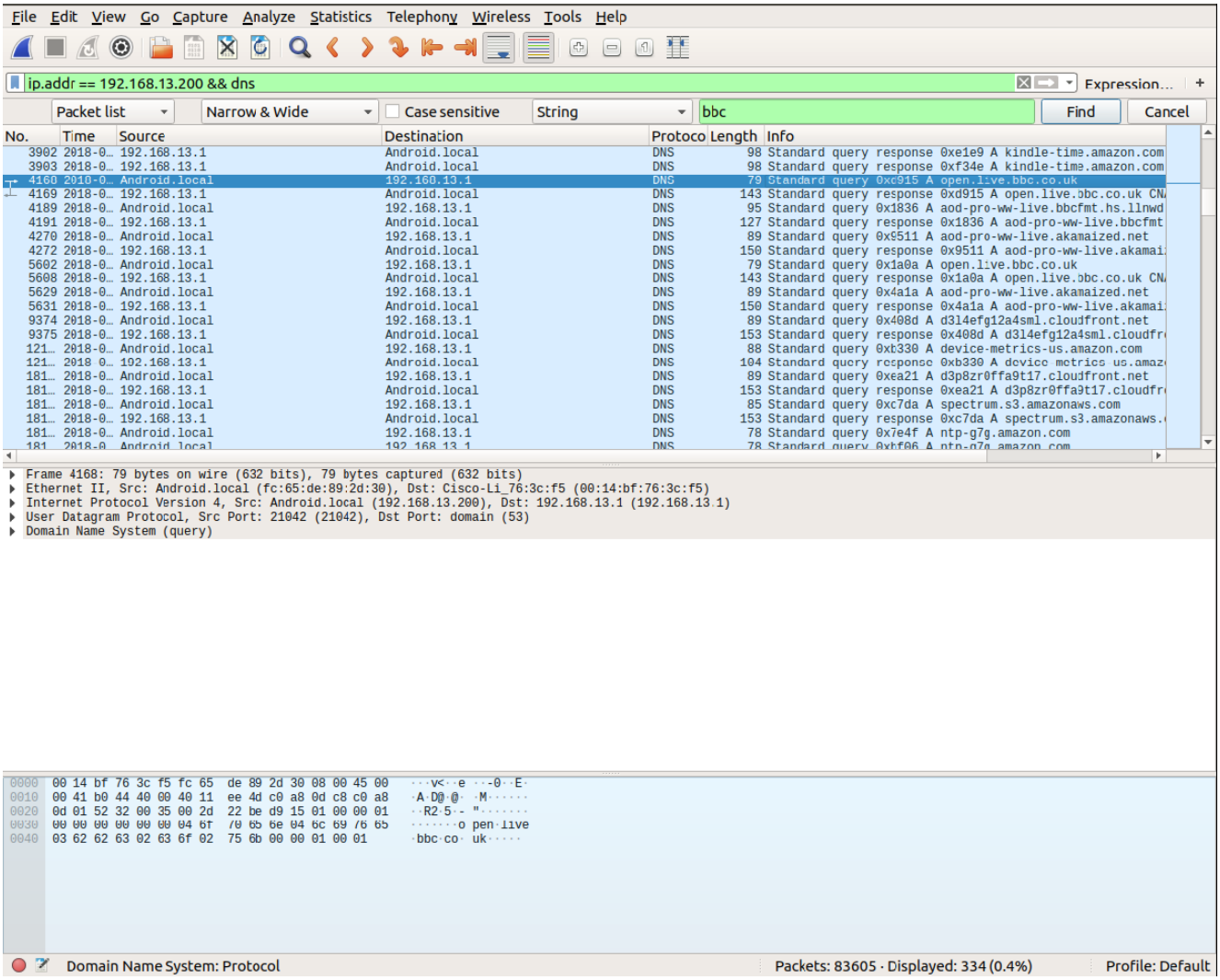

Fig. 2: Casting BBC news

Phone access). From a trust perspective, it requires the user to trust the app with access to basically every personal data the smartphone possesses.

Only the HO can visualise and control the historical data of the AED through the app. Moreover, the other users are not allowed to control the lights or other devices connected to the AED. We believe the design of the Amazon App is more restricted and the app does not trust the other users as much as the GHM's Home App.

Home App The Home app is designed to work in the presence of GHM devices, as opposed to the Alexa app, which can work as a standalone application, so it asked less permissions from our Android smartphones (only Contacts and Location).

The Home app restricts access to the GHM to all the users on the same Wi-Fi network (HO, HM and HG), so the HM is considered trusted and is able to use his Home app to access the device.

However, the HM must pair his device with GHM first. Then, the range of activities that the HM is allowed to perform is broad: he is able to see the current activity, cast songs (play, pause and stop any song playing), 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. Regarding the HG, he must not be able to perform any action because he is not supposed to pair with the GHM using the app. However, if the HG has paired another GHM (i.e. his GHM) and it is connected to the HO and HM's Wi-Fi, the HG is able to perform the same activities that HM can perform [17]. This aspect of the Home App is questionable from a security standpoint and can cause many privacy violations. In fact, in the event of the

[17]https://support.google.com/googlenest/answer/7177221?hl=en

HM or HG turning malicious, 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 use access to the HO calendar to perform malicious activities. In order to legitimate share the access of the GHM, the HO can add another user by their email address or a user on the same Wi-Fi network can send a request to take full control of the device. For any given request, the HO is able to accept or refuse the full access. However, even if the owner refuses the request, a user (i.e. HM, HG or MU) is still able to access the device and perform the actions that we mentioned earlier [18].

Hue App The Philips Hue lights gives access only to the owner of the house to control the lights through the Hue app with an authenticated account.

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 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 (i.e. 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.

Finally, by observing Hue network traffic, we noticed that the information generated by controlling the lights using the apps was encrypted.

D. Access Control Sharing

Amazon Echo The Alexa app restricts access to the AED 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. As a result, both the smartphones of the HM and HG are unable to check/control the AED device through their Alexa app. Amazon recently announced an app update to allow other users to share their AED [19]. However, the procedure does not look straightforward as it relates to the shared Amazon Account Households [20].

Google Home In order to share the access of the Google Home Mini, the owner can add someone using their email address or a user on the same Wi-Fi can send a request to obtain complete control of the device. For any request, the owner can accept or refuse access. In any case, even if the owner refuses a request, the user requesting could continue to have limited access to the device casting sounds or lowering/raising the volume. In addition, GHM has a guest mode in which a user that does not know the password of the Wi-Fi (i.e. the HG) can still cast audio/video to the device. All this user needs to do is request access to the guest mode in the Home app. To successfully connect to the device, the user has to enable the Wi-Fi sensor and have the microphone turned on and insert the correct PIN to be able to cast. The PIN is a 4 digit number that the Google Assistant will say out loud when it receives a request for guest mode access. If the microphone of the phone picks up the sound, then it is automatically authenticated. If it does not, then the user needs to insert it manually.

Philips Hue Lights The owner can share access to the lights providing the email address of the sharing user within the Hue app. This user needs to have that email address registered as a Hue account in order to be able to access the device. Anyway, this method is bypassed by the following one. In fact, if the HO gives the complete control of the GHM to another user, then that user will be able to control the Hue lights using his Google Home app even if he has not a Philips Hue account.

In Table III, we can see a resume of the functionalities described in Section III. Where there is the * symbol, it means that the answer is the one selected but with some possible restrictions. For the third functionality related to PHL, the answer is negative because it is mandatory to press the button and we assume that during the initialization phase only the HO is configuring the device and it is next to it. The same explanation is for the fourth functionality. About the voice recognition aspect, it is *Yes** for both AED and GHM because it is possible to configure it, but not by default. The ninth functionality related to GHM is *Yes** because even if the HO does not share complete access, a HM will be able to check what the device is casting even without complete access as we explained eralier. Finally, for the tenth functionality, the light access can be shared with the other users only if a complete access is provided by the HO.

TABLE III: Google Home Mini, Amazon Echo Dot and Philips Hue Lights comparisons

Functionality	**AED**	**GHM**	**PHL**
1) Account Authentication	Yes	Yes	Yes
2) Wireless Access Point	Yes	Yes	No
3) First configuration (anyone can become HO?)	Yes	Yes	No*
4) Later configurations (Only the HO?)	Yes	No	Yes*
5) Voice Interactions	Yes	Yes	No
6) Voice Recognition	Yes*	Yes*	No
7) App Interactions	Yes	Yes	Yes
8) Standalone App	Yes	No	No
9) Shared Complete Access	No	Yes*	Yes
10) Shared Lights Access	Yes*	Yes*	Yes

[18]https://support.google.com/googlenest/answer/9155535

[19]https://www.pcmag.com/feature/363112/how-to-let-multiple-people-use-the-same-amazon-echo/1

[20]https://www.pcmag.com/feature/335949/16-things-to-know-about-amazon-prime/7

IV. Trust Model for Smart Homes

Based on the experiment shown in Section III, we can devise two types of models: device to device models (D2D) and human to device (H2D) models. Even if the D2D model can be initiated by a voice command (i.e. "Alexa! Switch on the lights!") it is possible to create skills that can control the lights following specific rules (i.e. to switch always on the lights after the sunset), in this case, the communication is purely D2D. In any case, the trust model can be applied to both of these paradigms.

Moreover, we have identified four layers representing the relationships among devices and humans. The upper layer is the level 1. In this level, we identify the human users (i.e. owners, guests, malicious users). Then, the second layer is the level 2, where we identify smartphones that often have applications that allow control of the smart devices. Smartphones are usually controlled by humans belonging to the upper layer. We split humans and smartphones into two different levels to reflect the difference between app and voice interactions. In addition, it is possible that the smartphone checks the smart devices automatically (we do not consider in this paper the possibility that a malware inside the smartphone or the IoT devices could control the smart devices [23]). The third layer is the level 3 and it is composed of smart speakers (i.e. Amazon Echo and Google Home). Finally, the fourth layer contains all the smart devices that can be controlled by smart speakers, smartphones and humans (i.e. the Philips Hue lights). We can summarize that the layers 1 and 3 are a subset of the network related to the voice interaction showed in Section III-C1. The subset related to the app interaction is composed of the layers 2, 3 and 4 as shown in Section III-C2.

In summary, we can state that there is a trust and a control flow that can be identified moving through the four layers. The control flow follows a top-down direction. Thus, the set of the devices (or humans) belonging to a layer can control only the layers below and, for these devices, it is not possible to control the devices belonging to the same level or the levels above. On the other hand, the trust flow is directed following a bottom-up direction. In fact, trust is necessary among devices to be controlled by other devices or humans. The layers and the flows are shown in Figure 3.

These flows are very important in order to define the proposed trust models and how it should be applied. In Figure 3, we represent only the three allowed users avoiding the MU.

A. Human to Device (H2D)

We have identified two possible interactions involving humans and devices. In fact, a user can interact with AED, GHM and PHL by smartphone or by voice (in this case only with AED ang GHM). As stated before, a user (i.e. HM) can control the other devices or check them for updates using his voice. Restrictions can be applied by activating voice recognition or setting different user roles. In any case, if a HM can perform a voice interaction with the device, it means that he is in the same room as the device, so he might be trusted enough to perform actions. A solution to avoid improper accesses by voice is already possible configuring the voice recognition even if it implies possible privacy issues (i.e. users' voice will be stored and used for other purposes?). Thus, we do not propose modifications related to this aspect, we focus instead on the app interactions.

For most applications, the only requirement to be able to connect to the smart home devices is for the smartphone to be registered in the same Wi-Fi network as the devices. This means that it is possible to be connected even if the user is in another room or in a nearby flat. Such access allows other users to check the device's current activity and even interact with it (i.e. for GHM), as we presented in the previous Sections.

In the following subsections, we present the relationships among the humans using smartphones and the devices.

1) Smartphone - AED: The trust model associated to the use of the AED can be considered robust. To set the device, it is necessary to have an official Amazon account and only the HO is able to perform actions and check historical activities. However, there is an issue belonging to this phase. In fact, when the device is switched on for the first time, any user can take its ownership. An approach similar to the one implemented by PHL could solve this issue. In the case the HO is able to configure the device, later it will be possible only for her to set a new Wi-Fi connection through the AWAP in the case that the previously configured Wi-Fi network is not available anymore (i.e. moving the device to another house). For AED, the only trusted user is the HO, since it is not possible for other users to check or interact with the device using their Alexa apps. This implementation can be considered too limited and we propose a trust model to mitigate the hardness of the actual AED trust model. As we mentioned earlier, we are aware that Amazon is releasing an update for AED in order to allow multiple users to use it, but it is difficult to set it in a proper way.

2) Smartphone - GHM: If the AED trust model can be considered restrictive in some aspects, we can state that GHM trust model is, by design choice, more open. For GHM, all the users belonging to the same Wi-Fi network are trusted, which means all of them can connect to the device through the Google Home app and are able to interact with the device. In addition, even if a HG is refused by the owner, he still has access to the streaming data and it is possible for him to perform some actions that can be harmful or annoying for the legitimate users (as we have seen in the Section III). Finally, everyone can set the Wi-Fi settings of the device using the GWAP, which would violate our proposed trust model presented in section IV-C. In fact, it appears every time the previously configured Wi-Fi network is not available anymore. But, differently from AWAP, GWAP is configurable by anyone in its range even if the device is paired to another user. This can be harmful, because it is possible for a malicious user to change the Wi-Fi network used by the device. If this happens, the legitimate users (HM) and the HO are not able to control anymore the device through the app, neither to control the paired devices through it, because they are connected to the HO Wi-Fi network nor to the newly configured one. In

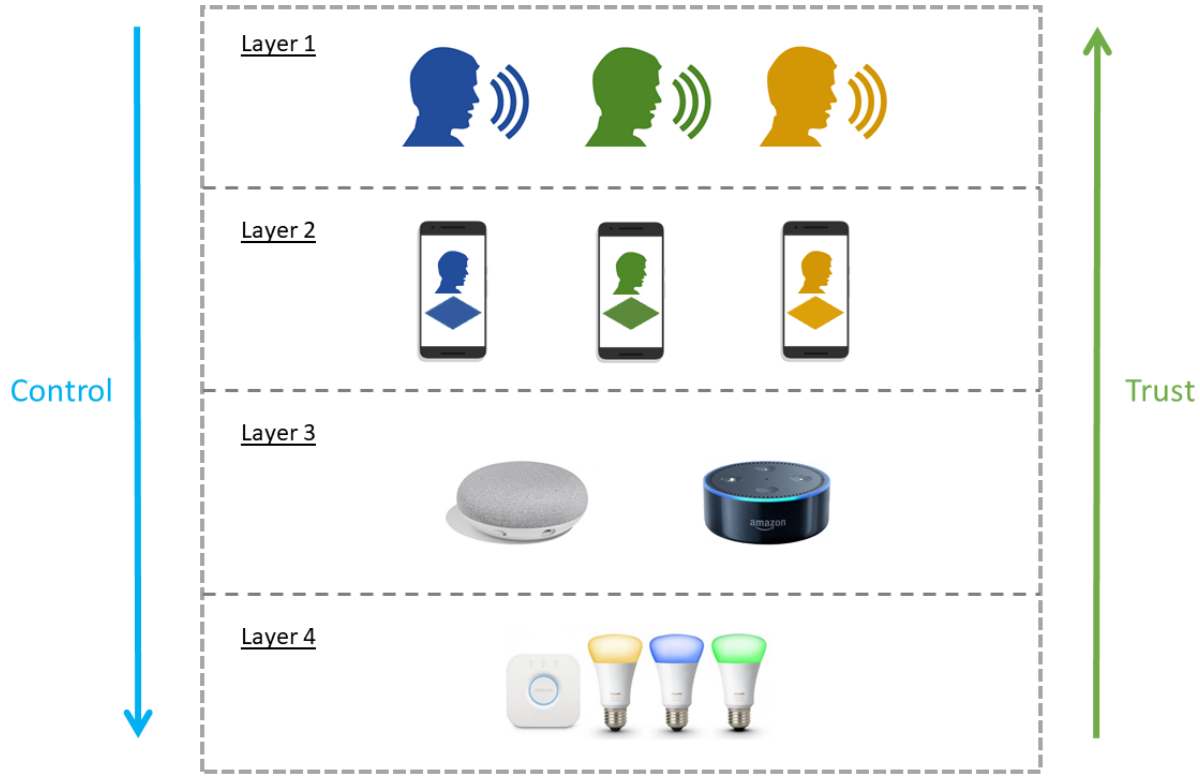

Fig. 3: Layers of trust and control

addition, because the Google Home can be a standalone device and it can be controlled only by voice, it is possible that the HO interacts with it without using the app. In this case, the HO could be unaware that the device is not connected anymore to her Wi-Fi network. In this way, a MU can take control of the device and restrict its use for legitimate users, even if this device is not in the same house. Thus, the MU could perform several malicious activities as we presented in Section III-C2. The only way for the HO to take again control of the device is to reset it, losing all the historical data and paired devices or to connect again to the GWAP in the case that the malicious user Wi-Fi network goes down.

3) Smartphone - PHL: The trust model related to PHL is simple to describe. Physical access is needed to the Hue Bridge and the users need a Hue account to configure it. Once configured by a user (i.e. HM), he can use the lights with his Hue app. In this case, the Hue Bridge will trust the device and with a proper configuration in the Hue website, it is possible to control the lights even from the outside. Regarding security and privacy, we can state that if a MU is sniffing the network, it is possible to understand if the user is at home or not by checking the communication between the IPs (even though the traffic is encrypted) [22]. The device will trust the communication because it will be received from the legitimate user. To enhance this protection, it could be useful to use always the cloud even if the user is using the same Wi-Fi network, but this approach can raise other issues (i.e. response time, more trust in the cloud).

B. Device to device (D2D)

In this case, we consider only the interaction among the smart speakers belonging to layer 3 and the Philips Hue lights belonging to layer 4.

1) AED/GHM - PHL: The direction of control is only pointing from AED and GHM to PHL. After the devices are paired, it is possible to switch on or off the lights directly using both voice commands or Alexa and Google applications. In such events, the communication is through the Hue Cloud, so it is not possible to sniff the packets and intercept the communication among AED or GHM and PHL. Nevertheless, the communication coming from the cloud is encrypted, thus it is not easy to understand the value. Even if the app is used to switch on or off the lights, the values are encrypted too as we show in Figure 4. In this figure, only the communication between GHM and PHL is represented, although the communication between AED and PHL is basically the same. A possible improvement, in order to avoid the cloud communication, was developed by Ferraris et al. [7] allowing different devices to share a key in order to exchange encrypted messages.

C. Proposed Trust Model

The set-up phase shows a limitation for both AED and GHM 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 GHM

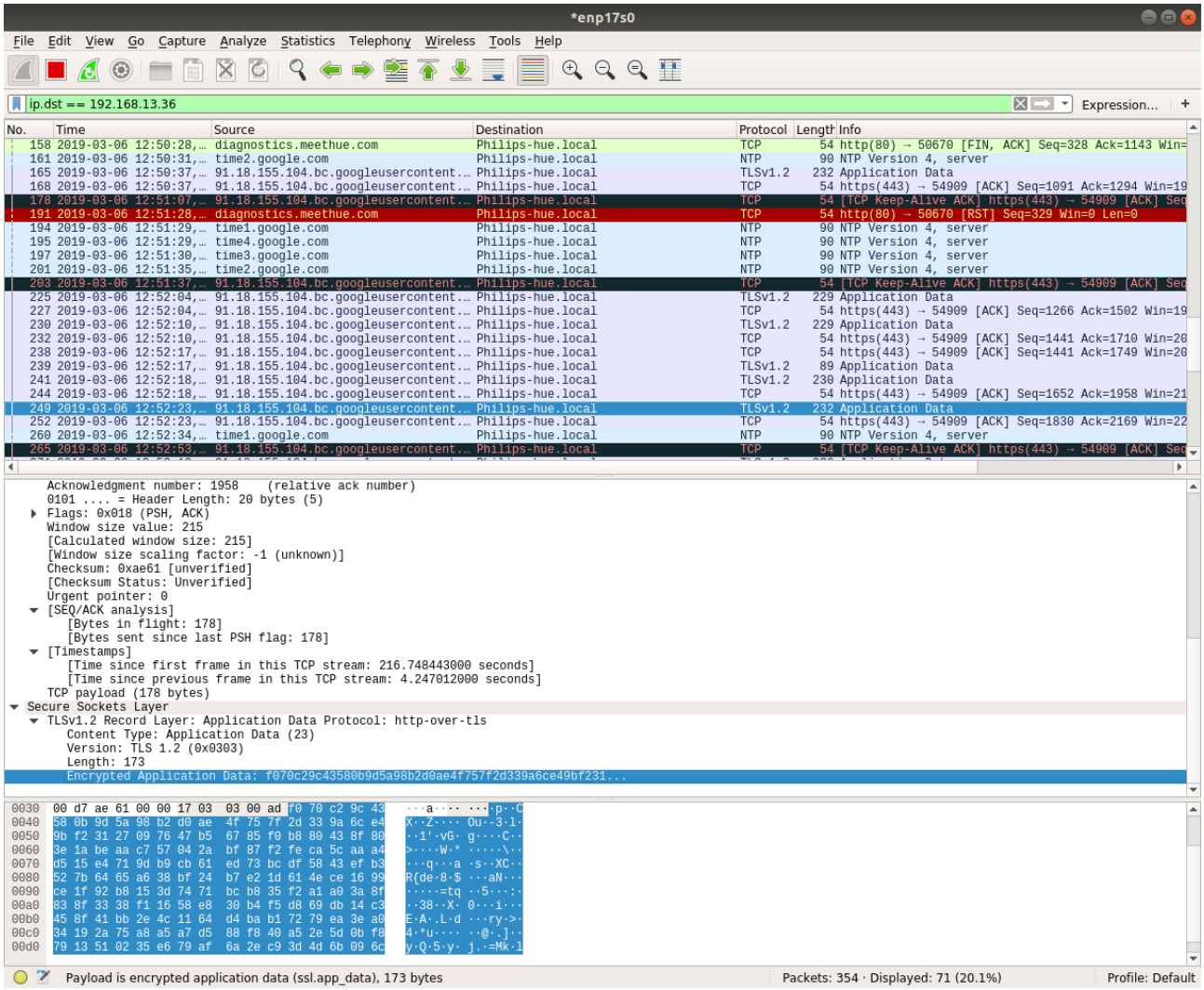

Fig. 4: Communication between Google Home Mini and the Hue lights

each time the GWAP appears. However, we can revert this by using the same approach used by AED (allowing only the HO to configure the device). For the AED 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 GHM allows the HM to control or check the device.

To solve these problems, we propose a trust model that uses a straightforward trust metric for each user, allowing them to use the devices according to that trust value. In this paper, we do not present a model for a centralized architecture because we did not consider a central hub. In our case study, there is a distributed architecture and we need to implement the trust models for each device. Considering Figure 3, we know that an entity (i.e. human or device) can only control the entities belonging to lower layers and the trust flow is pointing from the entities belonging to a lower layer to the ones of upper layers. In addition, only an enabled user or device must perform actions. Hence, we present the trust model using the following pseudo-code:

Algorithm 1 Trust model algorithm for home devices

```
1:  procedure TRUST CONTROL FLOW
2:      if device_belongs_to_upper_layer then
3:          if account_enabled then
4:              if trust_metric == high then
5:                  control_device;
6:              else if trust_metric == medium then
7:                  check_device;
8:              else
9:                  refuse_connection;
10:         else
11:             refuse_connection;
12:     else
13:         refuse_connection;
```

In the first step, the algorithm checks if the device belongs to an upper layer (in this case we need to implement the rules according to the architecture proposed). A possibility to detect whether a device is belonging to an upper or a lower layer can be achieved using different ranges of IPs according to the different layers. The process of choosing how to detect the layer of the device is a developers' task. If the device does not belong to an upper layer, the connection is automatically refused because a device cannot control devices on the same layer or the layers above. Otherwise, it is possible to proceed to the second step. Thus, the algorithm checks if the account is enabled. If it is not, the connection is refused, otherwise, the algorithm checks the trust value of the user. Then, there is a last check related to the trust metric and depending on its calculation it is possible to have three different trust levels: high, medium and low. The high level allows the user to control the device. The medium level allows checking the devices' activity but it denies control of the device. Finally, the low level means that the user is untrusted, so any connection must be refused.

The trust metric is composed of a score and a context value for each actor (user or device) having a role. The HO 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 the trust metric for each user.

1) Trust Metric: The trust metric is used to define rules for each actor and it is represented by the following function:

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

where the function $Trust\_Metric_x \in \mathbb{R}$ and its parameters are:

1) **Role (R)**. They have been presented earlier: HO, HM, HG and MU. For a D2D model the role will be related to the name of the device (i.e. AED).
2) **Context (C)**. It is related to the device or functionalities and its or their importance perceived by the HO.
   a) **Device/Functionality (DF)**. It is possible that a device has one or more functionalities. According to them and to the user involved, it is necessary to set the following parameters for each of them. We define them with natural numbers for both the device and the functionalities. Thus, we can have the device number 1 and 2 having several functionalities. For example, to represent the second functionality of the first device we will define the parameter DF as 1.2.
   b) **Context Importance (CI)**. It is related to the importance of the context according to the HO. 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. It is composed of two parameters: Device/Functionality (DF) and Context Importance (CI)
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}.

Regarding the roles, the HO is allowed full control of the device regardless of S and CI, given that she is fully trusted. For a MU, the metric works in the opposite way, since he is not allowed to control or check anything. In the case a HG or a HM turns into malicious, he will be treated as an MU and basically "banned". For this reason, we can state, that this model wants to reach two goals. The first one is to prevent any activities from an external user (i.e. MU). Then, the second goal is to be able to avoid attacks from internal users. If they happened the model threats the internal users as external ones preventing them to continue to use the device. Even for this role, CI and S are optional. On the contrary, for the other roles (HM and HG), CI and S are fundamental. The metric is plain and it is easily performed by any IoT device, even considering a limited computational power [19, 29]. It computes a value that will be used to check which actions are allowed for a particular user and for a particular context. It is basically a subtraction of the value S with respect to the value CI. 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 CI parameter 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 CI parameter has a value of 4, it means that is very important (i.e. to do bank transactions). Therefore, we can say that if a HM has a score of 5, he or she is similar to an HO, considering that with this score value it is possible to control everything, whatever CI is:

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

Conversely, if a user has a score of 0, he or she is considered as an MU and it is not possible to perform any actions (no matter the value of CI):

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

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 to perform actions. On the contrary, for an HO everything must be permitted. The values from 1 to 4 are used both for CI 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.

Now, we show some examples about the using of the trust metric:

$$Trust\_Metric_3 : TM(HM1, C(1.1, 4), 2) < 0$$

In $Trust\_Metric_3$, the user is a HM, the score is 2 related to the context (4) that it is higher. So, the computed trust level is low (lower than zero). This means that HM1 cannot perform actions because the score is lower than the context.

This can represent a scenario where the device can perform a bank transaction and HM1 is not trusted enough to do it. About the DF term we can define it as 1.1, representing the Device 1 (i.e. GHM) performing the functionality 1 (i.e. Bank Transaction).

$$Trust\_Metric_4 : TM(HM2, C(2.1,2),4) > 0$$

The contrary is presented in $Trust\_Metric_4$ where the computed trust level is high (greater than zero). This scenario can represent a high trusted HM and the context is related to switch on/off the lights. The parameter DF in this case can be represented by 2.1 where the device number represents PHL and the functionality the action to switch on the lights. For the sake of completeness, we present also $Trust\_Metric_5$ covering the action to switch off the lights.

$$Trust\_Metric_5 : TM(HM2, C(2.2,2),4) > 0$$

$$Trust\_Metric_6 : TM(HG1, C(3.2,3),3) = 0$$

In $Trust\_Metric_6$, the HG1 can only check the status of the device, in fact, the trust level is medium (equal to zero). This situation can represent a user allowed to check the calendar of the HO, but not to modify it. In this case the device is AED and the functionality 2 represents the calendar. We assume that the functionality 1 is the same related to GHM (i.e. Bank transactions).

$$Trust\_Metric_7 : TM(AED, C(4.1,3),1) < 0$$

Finally, in $Trust\_Metric_7$, we refer to a D2D interaction. In this case, the role is filled by the name of the device (AED). It is important to decide also if a device can perform a particular action in order to limit its possibilities even if previously the device has been allowed to perform the same action. In fact, our trust model can be implemented and then changed in the case that some modifications are needed. In this case, we assume that AED cannot open a smart lock (this device should be placed in the fourth layer of Figure 3) because its score is lower than the context. We assign the number 4 to the device (i.e. smart lock) and the functionality one is related to the action performed to open it.

2) Distributed vs Centralised: According to the example that we have proposed before, we can distinguish between a centralised or a distributed approach. We will expand the cases related to represented from $Trust\_Metric_3$ to $Trust\_Metric_6$.

In the distributed case, we have to store all the data related to the users and devices in the device itself.

In Tables IV, V and VI, we can see an example related to how the data must be stored in GHM, PHL and AED in order to be used in the trust metric presented earlier.

$Trust\_Metric_3$ is represented in Table IV (i.e. the first row), then we create several functionalities and we create the table according to another house member (i.e HM2) and a house guest (i.e. HG1).

The metrics take the data from the tables and compute them in order to allow or deny the users to perform the functionalities.

TABLE IV: GHM table

R	DF	CI	S
HM1	1.1	4	2
HM1	1.2	4	3
HM1	1.3	3	2
HM1	1.4	2	4
HM2	1.1	4	4
HM2	1.2	4	2
HM2	1.3	3	5
HM2	1.4	2	3
HG1	1.1	4	2
HG1	1.2	4	1
HG1	1.3	3	1
HG1	1.4	2	2

TABLE V: PHL table

R	DF	CI	S
HM1	2.1	2	4
HM1	2.2	2	4
HM2	2.1	2	4
HM2	2.2	2	4
HG1	2.1	2	1
HG1	2.2	2	1

$Trust\_Metric_4$ and $Trust\_Metric_5$ are represented in Table V (i.e. rows 3 and 4) and $Trust\_Metric_6$ is represented in Table VI (i.e. row 8).

On the other hand, in a centralised approach, we need to have a central hub, as proposed in [7], that can store information related to all the users and all the devices and their functionalities in different tables. Let us assume that we can store information in tables related to the users. We consider the following Tables VII and VIII. The tables refer only to the house members.

As we stated earlier, our trust metric is straightforward, but we need to store the data according to each user and each functionality. Thus, we can state that the complexity

TABLE VI: AED table

R	DF	CI	S
HM1	3.1	4	2
HM1	3.2	3	3
HM1	3.3	2	3
HM2	3.1	4	2
HM2	3.2	3	4
HM2	3.3	2	2
HG1	3.1	4	1
HG1	3.2	3	3
HG1	3.3	2	1

TABLE VII: HM1 table

DF	CI	S
1.1	4	2
1.2	4	3
1.3	3	2
1.4	2	4
2.1	2	4
2.2	2	4
3.1	4	2
3.2	3	3
3.3	2	3

TABLE VIII: HM2 table

DF	CI	S
1.1	4	4
1.2	4	2
1.3	3	5
1.4	2	3
2.1	2	4
2.2	2	4
3.1	4	2
3.2	3	4
3.3	2	2

of the tables grow according to the number of users and functionalities of each single device. Moreover, we can affirm that for each IoT entity, if the number of functionalities grows, the computational power must also grow.

For this reason, we can assume that if a device has a lot of functionalities to be performed, the same device can store a higher amount of data in respect to a device with limited functionalities and limited computational power. On the other hand, a device with limited capacity will require less data to be stored.

If we consider a centralised approach, we can store a higher amount of data, but we need to consider other issues (i.e. how to protect the communications among devices or to better protect the central hub) as presented in [7].

For all these reasons, we conclude that a distributed approach is preferable to a centralised one in order to use our proposed trust model.

V. Related Work

The IoT allows smart devices to be used through the Internet anywhere and anyhow [28]. These devices need to be secured through the Internet and they need to trust the other devices in order to interact with them [36].

According to Moyano et al. [20], 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". Through this definition, we understand that when there is a trust interaction, we have to consider basically two actors: a trustor and a trustee. The trustor is the actor needing the trustee to fulfill an action [9]. For this reason, trust is necessary between them in the whole interaction. In fact, trust is fundamental to decide which trustee is better to consider, to start the interaction and to accept the outcome as trusted.

Trust is strongly related to security in Information Technology [13, 15, 26] and also in the IoT field [8]. About it, Bastos et al. [2] identified several security risks in IoT technologies and protocols for smart home and smart city environments.

Trust in an IoT architecture is strictly dependent on how it is built [11]. Roman et al. [29] identified four type of architectures: centralized, distributed, collaborative IoT and connected Intranets of Things. Focusing on the first two types of architectures, we can state that a centralized approach is based on a central unit (i.e. a smart hub) that controls and allows other devices to interact. The smart hub is a single point of failure so it should be highly protected. Using this type of architecture, Ferraris et al. [7] proposed a segregated network that protect home devices and allow them to interact in a trusted environment, this is even more important in the case, for instance, of health monitoring services [33]. On the other hand, a distributed approach avoids the single point of failure delegating rules and powers directly to the edge nodes. Anyway, these edge nodes are not enough protected as the central unit of a centralized approach. Furthermore, the smart devices actually do not have enough computation power to protect themselves in an efficient way [29].

In addition to security and trust, privacy is another very important topic in IoT. Nieto et al. [21] investigated how privacy is related to IoT forensics and how the customers may be informed on which data could be stored and used. How the IoT devices and especially voice assistants keep trace of the data is not yet deeply investigated.

Nowadays, there is only a few research works on the security of the relationship among smart home devices, voice assistants and the end users [14, 24]. Chung et al. [4] apply the digital forensic approach to Amazon Alexa ecosystem combining cloud and client forensics. They proposed a tool supporting identification, acquisition and analysis for Amazon Echo devices.

Considering Amazon Alexa, in [3] 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 and they do not propose a solution. Furthermore, in [18] the authors investigated the security threats related to the voice commands and how the device accept them trusting any user is performing this action.

Considering smart home devices, Notra et al. [22] proposed a solution to protect devices such as Hue Light Bulbs, Nest Smoke Alarm and WeMo Motion Switch by restricting access at the network level. They stated that it is hard to standardize a security implementation into the IoT devices due to the heterogeneity of vendors, so they proposed a cloud service to guarantee Security as a Service (SECaaS). Although this is an interesting work, trust is not taken into account and security issues are still present in the cloud component. In addition, Zhang et al. [38] proposed a survey and a mitigation of the security risks about voice-controlled third-party skills built for amazon alexa and google home devices. Considering the difficulty to implement security and trust in an IoT device, Ferraris et al. [8] proposed a framework to develop Smart IoT entities in a standardized way. Through all the phases of the System Development Life Cycle trust such as privacy and security must be considered.

Taking a malicious user perspective, Ronen et al. [30, 31] performed cyber attacks against the Philips Hue light bulbs. They took advantage of a vulnerability through the radio protocol called Zigbee that is used for the communications among the Hue bridge and the light bulbs. The first attack was related to use the data captured by the lights from more

than a hundred meters of distance. The second attack was altering the frequency of the light (dangerous for people suffering epilepsy). However, they failed to show how the communication between the devices was performed. We will consider also the clear information that is possible to spoof during the devices communication.

In our work, we introduce a trust model capable of addressing the identified issues in the studied smart home devices. Our model is needed because the others presented in this section neither consider the different contexts nor the possibility to give a specific rank to different users. Even the trust models used by the aforementioned devices are either too much strict or too much permissive. With our solution, we gave the HO the possibilities to decide which functionality is possible to share with whom, allowing the possibility to consider trust holistically in the smart devices.

VI. Conclusions and Future Work

In conclusion, our study reveals that security is being taken seriously by big name manufacturers. However, by adopting our new trust model proposed in this paper, security could be improved in regards to how devices interact with users and other devices. The devices tested did not show basic security issues like default credentials or open *ssh* and *telnet* ports. We found that the Amazon Echo Dot approaches security in a restrictive way, providing the owner of the device tight control over who interacts with it and not making any trust assumptions. On the other hand, the Google Home Mini provides a more open approach by allowing any user on the same Wi-Fi network to interact with the device and cast media content. This reveals some trust assumptions. Hence, based on the analysis in [24, 38] and the trust model proposed in this paper, Google Home has a potential security issue that could allow unauthorised users who have gained access to home Wi-Fi network to perform activities like disabling previously set alarms. Finally, we investigated Philips Hue Lights and presented some issues related to its use in conjunction with the smart speakers. To address these issues, we proposed a trust model that achieves a responsible balance between the openness of Google Home and the limitations of Amazon Echo. Through 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 it still allows responsible sharing of the devices with other users.

For future work we plan to expand the number of tests on these devices and explore other privacy and security implications. In addition, we plan to add other smart devices to our testbed to achieve a more complex smart home ecosystem. We will give preference to devices supported by OpenHAB[21] in order to implement our trust model. These developments will allow us to expand our trust model as well as the threat model. Finally, the new relationships created by the newly added smart devices will help in order to validate the benefits and performance of our trust model.

[21] https://www.openhab.org/

Acknowledgement

This work has been supported by the EU project H2020-MSCA-RISE-2017 under grant agreement No 777996 (SealedGRID) and the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu).

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.

Compliance with ethical standards

Conflict of interest

All authors declare that they have no conflict of interest.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Aufner, P. (2019). The IoT security gap: a look down into the valley between threat models and their implementation. International Journal of Information Security, 1-12.

[2] Bastos, D., Shackleton, M., El-Moussa, F.: Internet of things: A survey of tech- nologies and security risks in smart home and city environments. IET Conference Proceedings pp. 30 (7 pp.)-30 (7 pp.)(1) (January 2018)

[3] Chung, H., Iorga, M., Voas, J., Lee, S.: Alexa, can I trust you? Computer 50(9), 100 (2017)

[4] Chung, H., Park, J., Lee, S.: Digital forensic approaches for amazon alexa ecosystem. Digital Investigation 22, S15-S25 (2017)

[5] Erickson, J.: Trust metrics. In: Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on. pp. 93-97. IEEE (2009)

[6] Fernandez-Gago, C., Moyano, F., Lopez, J.: Modelling trust dynamics in the internet of things. Information Sciences 396, 72-82 (2017)

[7] 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)

[8] 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)

[9] Ferraris, D., Fernandez-Gago, C. TrUStAPIS: a trust requirements elicitation method for IoT. International Journal of Information Security 19, 111-127 (2020). https://doi.org/10.1007/s10207-019-00438-x

[10] Ford, M., & Palmer, W. (2019). Alexa, are you listening to me? An analysis of Alexa voice service network traffic. Personal and Ubiquitous Computing, 23(1), 67-79.

[11] Ganchev, I.; Ji, Z. & O'Droma, M. A generic IoT architecture for smart cities IET, 2014
[12] Giesler, M., Fischer, E.: Iot stories: The good, the bad and the freaky. GfK Marketing Intelligence Review 10(2), 25-30 (2018)
[13] Hoffman, L.J., Lawson-Jenkins, K., Blum, J.: Trust beyond security: an expanded trust model. Communications of the ACM 49(7), 94-101 (2006)
[14] Hoy, M. B. (2018). Alexa, Siri, Cortana, and more: an introduction to voice assistants. Medical reference services quarterly, 37(1), 81-88.
[15] Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision support systems 43(2), 618-644 (2007)
[16] Jose, A. C., Malekian R. Smart home automation security: a literature review. SmartCR 5.4 (2015): 269-285.
[17] Kepuska, V., & Bohouta, G. (2018, January). Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home). In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 99-103). IEEE.
[18] Lei, X., Tu, G. H., Liu, A. X., Ali, K., Li, C. Y., & Xie, T. (2017). The Insecurity of Home Digital Voice Assistants–Amazon Alexa as a Case Study. arXiv preprint arXiv:1712.03327.
[19] Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (iot) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). pp. 336-341. IEEE (2015)
[20] 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)
[21] Nieto, A., Rios, R., Lopez, J.: Iot-forensics meets privacy: towards cooperative digital investigations. Sensors 18(2), 492 (2018)
[22] 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)
[23] Ozawa, S., Ban, T., Hashimoto, N., Nakazato, J., & Shimamura, J. (2020). A study of iot malware activities using association rule learning for darknet sensor data. International Journal of Information Security, 19(1), 83-92.
[24] Park, M. J., & James, J. I. (2020). Preliminary Study of a Google Home Mini. arXiv preprint arXiv:2001.04574.
[25] Park, J. S., Moon M., Hwang S., Yeom K. CASS: A
[26] Pavlidis, M.: Designing for trust. In: CAiSE (Doctoral context-aware simulation system for smart home. 5th ACIS International Conference on Software Engineering Research, Management & Applications (SERA 2007). IEEE, 2007.
Consortium). pp. 3-14 (2011)
[27] 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)
[28] Roman, R., Najera, P., Lopez, J.: Securing the internet of things. Computer 44(9), 51-58 (2011)
[29] 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)
[30] Ronen, E., Shamir, A.: Extended functionality attacks on iot devices: The case of smart lights. In: Security and Privacy (EuroS&P), 2016 IEEE European Sympo- sium on. pp. 3-12. IEEE (2016)
[31] Ronen, E.; Shamir, A.; Weingarten, A.-O. & O'Flynn, C. IoT goes nuclear: Creating a ZigBee chain reaction Security and Privacy (SP), 2017 IEEE Symposium on, 2017, 195-212
[32] Sciuto, A., Saini, A., Forlizzi, J., & Hong, J. I. (2018, June). "Hey Alexa, What's Up?" A Mixed-Methods Studies of In-Home Conversational Agent Usage. In Proceedings of the 2018 Designing Interactive Systems Conference (pp. 857-868).
[33] Shayesteh, B., Hakami, V., & Akbari, A. (2020). A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. International Journal of Information Security, 19(1), 93-110.
[34] Voigt, P., Von dem Bussche, A.: The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing (2017)
[35] Wiederhold, B. K. "Alexa, Are You My Mom?" The Role of Artificial Intelligence in Child Development. (2018): 471-472.
[36] 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)
[37] Ye, Mengmei, et al. Security analysis of Internet-of-Things: A case study of august smart lock. 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2017.
[38] 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. arXiv preprint arXiv:1805.01525.