*Journal of the International Society for the Systems Sciences | 66th Meeting of the International Society for the Systems Sciences*
*J.M. Wilby, Editor*

# LISTENING TO THE AFFECTED: SECURITY IN A HOME AREA NETWORK

**K.T. Nshimba**
Computer Systems
Vaal University of Technology, RSA
**Roelien Goede**
Unit of Data Science and Computing
North-West University, RSA

**Abstract**
With the advent of smart appliances and objects, a smart home has never been this complex. Today's homes are equipped with all kinds of smart objects capable of internet connectivity. Just a few years ago, a Home Area Network (HAN) only had personal computers and mobile devices making up the network. Today the picture is different, fridges, televisions, coffee machines, air conditioners, thermostats, and gate motors, just to name a few, are all capable of communicating with each other and on the Internet. This interconnectivity of various systems introduces a level of complexity to a home area network. For instance, these smart appliances and objects might be using different communication protocols, since each manufacturer may implement security differently. With the lack of standardization when it comes to the Internet of Things (IoT), this complexity opens loopholes in the security of the smart home.
By looking at a smart home as a complex system made up of sub-systems that may impact the security of the whole network, Systems Thinking will be a suitable approach to address this problem. Systems thinking was developed to address the complexity created by the interdependency of various systems, both existing and new ones.
In this paper, we propose addressing the data privacy issues of smart homes by looking at the problem from a systems thinking perspective. With this perspective in mind, we can address the security problems in a smart home by looking at it as a complex system. We relate the smart home as a system to Churchman's definition of a system as *a set of parts coordinated to accomplish a set of goals.* In this research, Critical Systems Thinking has been adopted as the preferred methodology for this research.

**Keywords**: Critical Systems Thinking, Systems Thinking, Smart Homes, Home Area Networks, Internet of Things (IoT), Data Privacy

## 1 Introduction

The adoption of smart technologies in homes around the world is gaining momentum. By 2022, it was estimated that around 130 million households will have one form or another of a smart object (Armstrong, 2022). This number is estimated to be around 335 million in just five years.
When we refer to smart technology in this paper, we consider various categories such as smart appliances, smart security equipment, and all other internet-enabled devices found in users' homes. Thus, the term Internet of Things (IoT) may be used to encompass all these Internet-enable devices found in a smart home. The term smart home as used in the literature, refers to a home that is

within a home area network (HAN) with Internet connectivity and giving an environment where these IoT devices are able to communicate with one another and to the Internet as well. Despite the convenience brought about by a smart home, it brings about the challenges of data security. Having a smart home is a balancing act for householders, on one hand these devices provide convenience, on the other hand they can put users at risk (Vogel, 2022).

The purpose of this paper is to consider the issue of data privacy and security of a smart home from a Critical System Thinking (CST) perspective. The focus is on how the decisions made by others, such as IoT device manufacturers (the involved), affect normal homeowners (the affected). CST is used to address complex problems that involve systems. In this paper, we look at a smart home as a complex system that comprises of other sub-systems. The rest of the paper is structured as follows; Section 2 provides literature-based discussions of the computer science concepts of the study namely Internet of Things (IoT) and computer security. Since Critical Systems Thinking is used to guide the methodology of the paper, a discussion thereof is provided in Section 3 aided by a demonstration of the characteristics of systems thinking IoT security. Section 4 provides a description of the methodology used. Section 6 the conclusion is presented.

## 2 Internet of Things and Privacy

The Internet of Things brings along many benefits for homeowners, but along with it comes data privacy, or the lack thereof. In this section a discussion of current and future IoT adoption rates and a brief outlook on the data privacy is given.

### 2.1 Internet of Things

The term IoT is used to describe categories of smart objects with the ability of its sensors to collect data from their environment, and then transmit that data to online servers for analysis. The interconnect capabilities of IoT devices make it easy to remotely control various functionalities of a smart home. Smart home technology has a high adoption rate. Figure 1 shows which smart device has seen greater adoption and the estimated numbers in just five years. By 2021 the global smart home market was estimated to be around 99.89 billion US dollars. By 2028 that number is expected to be around 380.52 billion US dollars, that is an estimated compound annual growth rate (CAGR) of 21.1%.

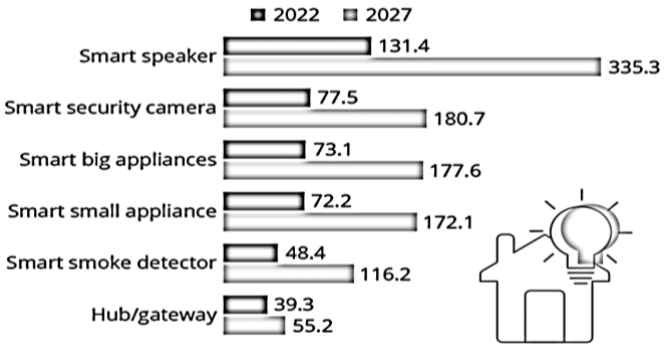


*Figure 1 Estimation of smart devices adoption worldwide (in million), (adapted fromArmstrong, 2022).*

When discussing smart homes in this paper, we are referring to a HAN that has devices that are equipped with computing capabilities. These devices are able to communicate with one another, able to collect (using various sensors) and transmit data, and they can be remotely controlled over the Internet (Bugeja, Jacobsson, & Davidsson, 2021). With the advancement in computing technology, more and more common household appliances are becoming smart. Appliances such as a smart fridge provide convenience that we never had before. Households can now check what they need in the fridge by just sending a query to the fridge to see if there is still milk or other products. Using Machine-to-Machine (M2M) communication, smart devices can be able to send commands to each other without user intervention when programmed with If This Then That (IFTTT).

### 2.2 Data Privacy and Security in Smart Homes

The introduction of IoT devices in one's home brings about convenience, but also security challenges. Some of these devices are equipped with powerful microphones, others have cameras. Although these sensors in themselves may not pose a risk, in the advent of them being hacked, they can be used to spy on unsuspecting homeowners. According to Kaspersky (2023), many smart objects being used in smart homes are easy to hack because they offer little protection. This is mostly due to poor security implementation in these devices. In a HAN, such a device can become an entry point for intruders. Any kind of vulnerabilities found in the security implantation of these devices can easily be exploited to mount an attack. Once an intruder is able to gain access to the whole network, all the other devices in the network are now easy to target. Intruders may steal identification or financial data. They can also be able to do harm by causing a smart appliance to malfunction for instance. It is therefore vital for homeowners to be aware of the risks posed by these devices.

## 3 Critical Systems Thinking (CST)

To achieve a shared understanding, this section provides some information on systems, systems thinking and critical systems heuristics.

### 3.1 Systems and systems thinking

Researchers have developed various frameworks to address problem-solving in different fields of study, including Social Science, Management Science, Engineering, and Information Technology. One approach to complex problem-solving is the application of Systems Thinking (ST). Before we look at ST in detail, let us first start by defining what a system is and how ST can be used in understanding it.

The earth is full of systems, both natural and manmade ones. For instance, the earth itself is one big ecosystem that is made up of larger and smaller eco-systems *(Geography, 2022*). Within each of these eco-systems, you find animals and plants that are systems in their own right. Every factor of such eco-systems influences other systems due to their interconnection. A system is defined as a "set of parts coordinated to accomplish a set of goals" (Churchman, 1968, p. 29). It is important to note that each "part" of a system can also be a system on its own. Thus, a system can comprise of other sub-systems. When trying to understand any system, it is vital to be familiar with its

environment, its objective, and what role each part of the system plays in supporting the overall objective of the system (Churchman, 1968, p. 29). In an ecosystem such as a forest for instance, each tree, animal, insect, fungi, worm etc., plays a vital role. Trees provide food for animals, in turn animals provide fertilizer for plants. When animals die, fungi play a vital role in decomposition thus keeping the forest clean of carcasses. The forest itself plays a vital role in providing shelter and food for animals, reducing carbon dioxide in the environment, and pumping more oxygen into the atmosphere. The forest itself becomes a part or sub-system, playing an important role in helping the earth, as a system, to support life.

According to Churchman (1968, p. 29), we need to keep five basic considerations when describing a system. These include the overall objective of the system; the environment of the system; resources of the system, components of the system, and management of the system. A system may have many objectives, but the real objective will be the one that will not be sacrificed in order to attain the system's goal *(Churchman, 1968, p. 31)*. For instance, a company using a production system for sanitizers may claim that the objective in increased production of sanitizers is to combat Covid-19, but their main objective might be increased revenue. According to Churchman (1968, p. 31), it is difficult to determine the real objectives of a system. This may be due to the fact that we might not be truthful about the real objectives. Due to this difficulty, it is better to rather make use of the overall performance measures of a system to see how it is doing (Churchman, 1968, p. 31).

The environment of a system can be described as anything has an impact on the system, but is not controlled by the system. The system does not have control over its environment, in essence the environment has some impact on the performance of the system, either positive or negative. For instance, returning the example of the company trying to produce more sanitizers to combat Covid-19, it might have happened during the lockdown that all cargo transportation systems came to a halt for weeks or months. This could have affected the delivery of raw materials and in the process slow down the production rate. There is really nothing the company could have done because it had no control of the situation.

Unlike an environment that a system has no control over, a system has control of its resources and can use them to their advantage in support of achieving the objective of the system (Churchman, 1968, p. 37). Resources are used by a system to control the various actions of the system. Resources may include workers, hardware, software, and more; basically, anything the system may utilize to its advantage in achieving its goals.

The term component can be interchangeably used as being a part or a sub-system. When describing a system, we can consider that the whole system is comprised of parts which contribute to the overall functionality of the system. Each of the parts may have a different role to play which, in turn help the system achieve its main objective. A component can also be described as a system with its own objectives, environment, resources, and even its own parts as well. Also, every sub-system can comprise of other sub-systems.

The management of a system brings everything together harmoniously. For instance, through management a system is allocating the required resources for a particular objective to be achieved, or the performance of the system to be monitored (Churchman, 1968, pp. 44-46). The management

plays the orchestration role in making sure every sub-system is able to reach its objective, which in turn helps the whole system in reaching its primary objective.
Arnold and Wade (2015, p. 675) define systems thinking as *"a set of synergistic analytic skills used to improve the capability of identifying and understanding systems, predicting their behaviors, and devising modifications to them in order to produce desired effects".*

If we can approach every complex problem as a system, we can therefore apply systems thinking methodologies to find a solution. Vital to this way of studying a system is that the whole emerges from the interactions of the parts (Jackson, 2003, p. 3). Holism also values the importance of each part and the relationship among these parts and the role they play in the emergence of the whole, but the main difference is that holism sees the whole as the most important part because it considers a system to be more than just the sums of its part (Jackson, 2003, p. 4).

### 3.2 Critical Systems Thinking

According to Jackson (2001:238), CST has aimed to collaboratively harness various methodologies, methods, and models from the field of management science. This collaborative effort involves assessing their underlying assumptions with the overarching goal of enhancing complex societal systems. CST was created primarily for the analysis of complex societal problems and the means to solve such problems.

Critical Systems Thinking has roots in both systems thinking and social theory, thus it has inherited concepts such as boundaries, relationships, and emergence from systems thinking, but also gained the strength systems theory has on the ontological and epistemological assumptions. Although both approaches have strength that CST has inherited from, they share a common weakness when it comes to practice.

Werner Ulrich is an important scholar in CST, his work in critical systems heuristics (CSH) (Ulrich, 1983) made a major contribution to the field. In this paper we will not use the full set of 12 questions known as critical systems heuristics. Our focus is on Ulrich's distinction between the involved and the affected in the problem situation. Ulrich (1983) describes the affected as those who must deal with the consequences of the decisions made by the systems planners. He argues that they should be represented in the system by a witness.

## 4 Application of the Systems Approach: Smart Home as a System

A systems approach can be used in explaining any complex system by breaking the system down into its parts and examining the functionality of each part and how their interaction affect the overall functionality of the system. In this section, we will look at a smart home as a system.
Network security is a complex task to achieve successfully, but we can divide the smart home's security into various components or sub-systems, we can then analyze how each of these sub-systems is contributing to the overall objectives of the smart home. Let us start by identifying a smart home and its sub-systems, then for each of the sub-systems we will identify its objectives, environment, resources, components, and lastly how all these are managed on a sub-system level.

We are now going to consider each sub-system of a smart home. For this research, we selected five categories of smart appliances and devices, namely smart fridges, smart speakers, smart locks, smart TVs and smart IoT gateways. This of course does not represent all the sub-systems of a smart home, but they are a good representation of the sub-systems.

A smart home can be a complex setup. We are going to look at it from the perspective of a system, as such we expect a smart home to conform to the five characteristics of a system described in section **Error! Reference source not found.**, in that it should have an environment, i.e., the HAN in which it resides; resources, i.e. electricity and network connectivity which are vital to its functionality; components, i.e. the various sub-systems that contribute to the functionality of the smart home, such as smart appliances and other smart objects; and lastly the means to manage all these sub-systems to help the smart home achieve its function.

### 4.1 Objectives of a smart home

We can think of a smart home as " *a residence equipped with a communications network, linking sensors, domestic appliances, and other electronic and electric devices, that can be remotely monitored, accessed or controlled and which provide services that respond to the needs of its inhabitants*" (Balta-Ozkan, Davidson, Bicket, & Whitmarsh, 2013, p. 362). With this definition in mind, we can now list the true objectives of a smart home as:

- to provide a secure environment for smart objects/devices to operate within,
- to provide data protection and privacy of homeowners,
- to provide convenience (Gram-Hanssen & Darby, 2018, p. 96) by services being offered by the various smart objects/devices, and
- to improve the quality of home life (Sovacool & Furszyfer Del Rio, 2020, p. 5) through the use of improved services and functionalities.

The objective of the smart home as a system can then be summarized as:

> The smart home is a collection of connected electronic devices aimed at improving the quality of home life by providing convenience of services in a secure environment which protects the privacy of the owner.

### 4.2 Environment of a smart home

As it was described above, the environment is anything that may be anything beyond the control of a system but has an impact on its operation. These may include service availability such as water, electricity (i.e. power outages) and network availability (i.e. internet outage). They may be other factors of human nature, such as intruders stealing anything that may disrupt power or network connectivity in a smart home.

### 4.3 Resources of a smart home

A smart home requires resources for it to provide the required functionality. These may include control software to manage IoT devices, applications to manage and provide security, Intrusion Detection Systems (IDS), Internet connectivity to allow remote management and transmission of data to and from cloud-based services.

### 4.4 Components of a smart home

As explained in the introduction, a system has parts or components, which can be considered to be sub-systems as well. Each of these sub-systems needs to have a goal, and activities they carry out, and we need to have the means to measure its performance. Every IoT device in a smart home can be seen as a component or part. Each of these devices can also be a sub-system in their own right, with their own environment, resources and the likes.

### 4.5 Management of a smart home

The management brings all four of the preceding characteristics together. Management of a system ensures resources are provided, and that the system performs well to achieve its objectives. Smart home technology providers offer various systems for managing a smart home. A centralized system can be used to manage all IoT devices, especially if they are from the same manufacturer. although each device may come with its own management system. For example, Samsung's SmartThings suite of applications provides a centralized management of IoT devices that are supported (Samsung, 2023).

In terms of the work of Ulrich (1983), the 'involved' are those parties who can direct the outcome of the decisions in the systems design process. In our project on the security of HANs, we view the manufacturers of the IoT devices as the involved and the homeowners as the affected in the system.

Manufacturers of IoT devices (the involved) make decisions that significantly impact consumers. Their decisions on how certain functions are implemented, such data privacy, may have no input from ordinary users (the affected). It is crucial to give ordinary users a voice, so they have knowledge of what kind of data is collected and how their privacy may be affected. This kind of knowledge will help homeowners become "experts of their own lives," making informed decisions when purchasing IoT devices. Education is key to empowering homeowners to become experts in their own decisions.

With this reflection in mind, we conducted an empirical study to identify the security threats of various smart home devices on the unsuspecting homeowners as "the affected" in the systems.

## 5 Methodology used in the Empirical Study

Putting yourself in the shoes of others is crucial in critical systems thinking. The research aimed to investigate security threats of smart home devices from two main groups, namely the manufacturers of IoT devices and the consumers. In order to understand the perspective of the manufacturers regarding their implementation of security and their handling of the data they collect, we analyzed manufacturers' documentation of our selected devices. In order to listen to the voice of the affected homeowners, we used security reviews of IoT devices to obtain data.

Using CSH terminology, we refer to the manufacturers as the "involved" since they make decisions that have an impact on users of these devices, and to consumers as the "affected". In order to have a better understanding of the manufacturers' implementation of security in these devices, we collected data from the manufacturers' technical manuals and technical reviews online for each

device. We used document analysis as a method to analyze and code the data from an interpretive research perspective. The categories we focused on were the threats and vulnerabilities of each device analyzed. For instance, Table 1 shows the method used to collect data from manufacturers. The data sample is for smart speakers, and for each device, motivation is given as the deciding factor. We collected data on the top three manufacturers, despite there being others in the market. In Table 2 and

Table *3*, coding was developed to represent the vulnerability and threat capabilities of these devices. In some cases, no detail was provided by the source, this is indicated as NC for No Comment in the tables.

*Table 1 Smart speakers data source*

| Model | Motivation for selection |
|---|---|
| **Echo** | By 2018, the USA alone had almost 118 million smart speakers in users' homes (Sterling, 2019). Amazon alone claims to have sold around 100 million Echo smart speakers worldwide (Leary, 2019). The Echo model seems to be the most popular smart speaker from Amazon. Also, Amazon is currently the leader in the number of smart speakers sold to date (Owen, 2019). |
| **Home** | Google Home is the second most sold smart speaker, according to published reports (Owen, 2019). By the end of 2018, almost 11 million google home smart speakers were sold. |
| **Homepod** | Apple Homepod is added to this list because Apple produces premium products. Although it might be 6th globally, it is 3rd in the USA, and the brand is well known also globally as compared to Chinese brands which are currently only popular locally. |

*Table 2 Representation of manufacturers' documentations (smart speakers)*

| **Manufacturers** | **Amazon** | | | **Google** | | | **Apple** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Model** | **Echo Dot** | | | **Home** | | | **Homepod** | | |
| **Codes** | **Yes** | **No** | **NC** | **Yes** | **No** | **NC** | **Yes** | **No** | **NC** |
| **VULNERABILITY** | | | | | | | | | |
| Acknowledges speaker having a microphone. | X | | | X | | | X | | |
| Acknowledges that the speaker is always listening. | X | | | X | | | X | | |
| Specifies how much RAM the speaker has. | | X | | | X | | | | X |
| Manufacturer specifies the type of encryption the speakers use. | | X | | X | | | | | X |
| Specifies the CPU being used by the speaker. | | | X | | X | | X[1] | | |

[1] Apple acknowledges that the smart speaker is using an A8 processor.

| **Manufacturers** | **Amazon** | | | **Google** | | | **Apple** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Model** | **Echo Dot** | | | **Home** | | | **Homepod** | | |
| **Codes** | **Yes** | **No** | **NC** | **Yes** | **No** | **NC** | **Yes** | **No** | **NC** |
| | | | | **THREAT** | | | | | |
| Acknowledges that the speaker is always listening. | X | | | X | | | X | | |
| Acknowledges collecting information on the usability of the service by users. | | | X | X | | | X | | |
| Acknowledges storing collected data from smart speakers on their servers. | X | | | X | | | | | X |
| Acknowledges storing a recording of voice commands to improve the functionality of the service. | | | X | X | | | | | X |
| Acknowledges encrypting conversations stored locally on the device. | | | X | X | | | | | X |

Our document analysis of the reviewer's comments which served as the voice of the affected was done using a content analysis strategy with coding methods from qualitative research. Table 3 provides a example of our data presentation.

*Table 3 Representation of manufacturers' documentations (smart TVs)*

| Manufacturers | SAMSUNG | | | LG | | | SONY | | |
|---|---|---|---|---|---|---|---|---|---|
| **CODES** | **YES** | **NO** | **NC** | **YES** | **NO** | **NC** | **YES** | **NO** | **NC** |
| **VULNERABILITY** | | | | | | | | | |
| Acknowledges a range of TV sets having a microphone. | X | | | | X | | X | | |
| Acknowledges a range of TV sets having a camera. | X | | | | X | | | | X |
| Acknowledges storing collected data on the TV set or in the cloud. | X | | | X | | | | | X |
| Acknowledges that not agreeing to the privacy policy document can limit the functionalities of the smart TV. | X | | | X | | | | X | |
| Specifies that disabling of personalized recommendations does not stop collection of data on the smart TV's usage. | X | | | | X | | | X | |
| Acknowledges giving collected data to third party companies for further processing. | | | X | | | X | X | | |
| Acknowledges not collecting and storing data on minors. | X | | | X | | | X | | |
| Specifies for how long they store the collected data. | | X | | | X | | | X | |
| Acknowledges collecting sensitive information from users. | X | | | | | X | X | | |
| Acknowledges collection of video footage via the camera on the TV. | X | | | | X | | | | X |
| Acknowledges collection of TV IP address and device ID by third party companies. | X | | | | X | | | | X |
| **Manufacturer specifies using encryption.** | X [2] | | | | X [3] | | | | |

[2] The TV set support WEP, WPAPSK, WPA2PSK authentication methods, and WEP, TKIP, AES encryption. Samsung advises users to connect their TV set to the wireless HAN using one of the encryptions methods.

[3] Although LG does not specify what encryption the TV supports, but they leave the decision to connect to a wireless network on the user. They suggest that if the access point uses any kind of security, then the user should enter this on the TV.

| **Manufacturers** | **SAMSUNG** | | | **LG** | | | **SONY** | | |
|---|---|---|---|---|---|---|---|---|---|
| **CODES** | **YES** | **NO** | **NC** | **YES** | **NO** | **NC** | **YES** | **NO** | **NC** |
| Manufacturer acknowledges presence of a LAN or Wi-Fi network card. | X | | | X | | | X | | |
| Acknowledges TV users can install apps from third party. | X | | | | | X | | | X |
| Manufacturer specifies using a CPU in the set. | X[4] | | | | | X | | | X |
| Manufacturer specifies what OS the TV is using. | X[5] | | | X[6] | | | X[7] | | |
| Manufacturer specifies how much RAM the TV set has. | X[8] | | | | X | | | X | |
| **THREAT** | | | | | | | | | |
| Acknowledges that unauthorized access can happen between the communication of the smart TV and company servers. | | | X | X | | | | | X |
| Acknowledges sharing of collected data. | X | | | X | | | X | | |
| Acknowledges using users' collected data. | X | | | X | | | X | | |
| Acknowledges collection of data via the set. | X | | | X | | | X | | |
| Admits collecting basic information, such as channels viewed, menu clicked, and apps accessed. | X | | | X | | | X | | |
| Admits collecting voice information via the TV set. | X | | | X | | | | | X |
| Specifies that marketing companies have abilities to connect to your TV set. | X | | | | X | | | | X |

[4] Samsung only gives mention of the fact that the set uses a quadcore CPU nothing more on the specifics.
[5] Although Samsung does not specify it in the TV manual, but they specify on their developer website (Samsung, 2019) that smart TVs are using Tizen OS.
[6] LG acknowledge that their smart TVs are using WebOS.
[7] Sony acknowledges that the TV set is using Android TV OS.
[8] Samsung argues that every TV set may have a different amount of RAM, but in their help documentation they specify the steps a user can take to view the amount of RAM.

| **Manufacturers** | **SAMSUNG** | | | **LG** | | | **SONY** | | |
|---|---|---|---|---|---|---|---|---|---|
| **CODES** | **YES** | **NO** | **NC** | **YES** | **NO** | **NC** | **YES** | **NO** | **NC** |
| Acknowledges the sale of user data to third parties. | | | X | | | X | | | X |
| Acknowledges sharing collected users' information with the authorities, such as the police, when required. | | | X | | | X | X | | |
| Acknowledges collecting sensitive information from users. | X | | | | | X | X | | |

Similar tables were created for other smart appliances. The full set of tables are outside the scope of this paper, but available on request from the author.

## 6 Findings and Conclusion

From the collected data, it has been observed that although manufacturers may not intentionally create IoT devices with vulnerabilities, the hardware and software compositions of these devices do present opportunities for bad actors to exploit them. As IoT is still a developing technology with extensive potential and use cases, manufacturers play a vital role in ensuring that built-in security in these devices is of paramount importance, ahead of profitability. However, how do we give a voice to ordinary homeowners who have no idea about the potential dangers of not understanding the technology and the looming threat that IoT devices pose to their data privacy in their homes?

The best way to empower homeowners to make informed decisions about the purchase and usage of IoT devices is through education. First, homeowners need to be educated on the basic security features that may come with the devices and what type of data is collected. This was accomplished by creating guidelines for homeowners.

As smart technology for homes becomes more adopted by homeowners, the number of security breaches will also increase. Therefore, guidelines on how users protect themselves and their homes will need to be revised from time to time to keep with the advancement of the technology and its adoption rate. These guidelines need to be dynamic as the technology changes and new threats are discovered, they will also need to be regularly updated. From our analysis we were able to list the following general guidelines for homeowners about the security threats of smart home devices:

- For each device in the smart home, be sure to understand the user interface, pay special attention to user access and authentication.
- For each device in the smart home, be sure to investigate which security settings can be configured by the user.
- When using a mobile app to configure devices, be aware of vulnerabilities caused by outdated software and lack of updates.
- Restrict access to mobile devices used to control the gateway.
- Always set the mobile app to update automatically.

- Ensure that smart device firmware is up to date.
- Be aware of the service level agreements in terms of data protection, encryption and sharing of data.
- Be aware of the security impact of the specific type of network used to upload data from the device to the cloud.
- Be aware of different types of networks used in smart homes and that the connection between devices may be insecure.
- Investigate which security and protocol settings can be controlled on the gateway to improve secure communication.
- Investigate which OS is installed on a gateway, the well-known OSs used in current mobile phones and tablets are typically more secure than an unknown one.
- Be aware of electricity options in terms of uninterrupted power supply of the hub since power cuts may be a form of attack.
- Be aware of the dangers concerning communication between the mobile app and the gateway for control. Investigate the encryption provided and ensure it is activated.
- Be aware of which sensors are installed in each device and which data they collect and importantly over what range they collect data.
- Investigate the effects when a specific sensor fails on the functionality and safety of the appliance.
- Be aware of the time settings of data collection and the reach of the sensors to know when and where data is collected.
- Investigate the OS used in appliance or host device to understand secure data storage and transfer from the specific device.
- Be aware that individual devices have identification tags that may be copied to create insecure entries.

Specific devices also require additional guidelines, which we provide in Table 4.

*Table 4 Additional device specific guidelines from empirical study*

| Additional Device Specific Guideline |
|---|
| **Television** |
| • Be aware that all additional apps loaded on the TV may pose additional security concerns. |
| • Users should be aware that they need much more knowledge than anticipated to protect themselves. |
| • Pay special attention to data collection and sharing in the policy documents of the specific manufacturer. |
| • Investigate the specific OS of a smart TV model. Different models of TVs use different operating systems, each with implications of security. |
| **Smart Speakers** |
| • Users should delete old data from the device. |
| • Access to the device in a smart home should be considered as a risk and therefore users should know the range of their speakers. |
| **Smart Locks** |
| • Users should consider everything that can go wrong if security attach is experienced. |
| • Users should use a qualified technician to install devices and discuss security concerns with them. |
| **Smart Fridges** |

- User access is of greater importance since the fridge can be used as the gateway. Users need to be aware that their IoT fridge maybe not be able to detect that it has been affected by malware, so extra precaution is needed to make sure they keep their appliances unaffected.
- Users should be aware that the durable lifespan of the fridge itself is much longer than that of technology. Support might not be available while the fridge is still working. This is especially a concern for security updates.
- When buying a fridge, a user should make himself/herself aware of all the security concerns of gateways.

**Smart gateways**

- User access is of great importance, since all other devices the home is connected to the gateway. The consequences of a possible attack concern every aspect of the network.
- Users need to be aware that the gateway is always watching cameras and always listening microphones. This also implies that users should know the ranges of these sensors.
- Users should take responsibility to know what is recorded and what is done with the data.
- Users should understand that secure network communication depends on hardware and OS capabilities of the gateway, as well as the continued support thereof in terms of updates.

By using a critical systems approach we were able to better understand the smart home as complex problem environment. We able to distinguish between the involved and the affected as well as the resources and the environment. The use of this boundary critique enabled us to structure our investigation.

Although it was possible to develop guidelines grounded in our data it is still a major challenge to inform the affected homeowners of the risks involves when turning their homes into smart homes.

## 7 References

Armstrong, M. (2022). Homes Are Only Getting Smarter. Retrieved from https://www.statista.com/chart/27324/households-with-smart-devices-global-iot-mmo/

Arnold, R. D., & Wade, J. P. (2015). A definition of systems thinking: A systems approach. *Procedia computer science*, *44*, 669-678.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). The development of smart homes market in the UK. *Energy*, *60*, 361-372.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2021). PRASH: a framework for privacy risk analysis of smart homes. *Sensors*, *21*(19), 6399.

Churchman, C. W. (1968). The systems approach, 1968. *A Challenge to Reason*.

Geography, N. (2022).

Gram-Hanssen, K., & Darby, S. J. (2018). "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science*, *37*, 94-101. doi:https://doi.org/10.1016/j.erss.2017.09.037

Jackson, M. C. (2003). *Systems Thinking: Creative Holism for Managers*. West Sussex, England: John Wiley & Sons, Ltd.

Kaspersky. (2023). How safe are smart homes? Retrieved from https://www.kaspersky.co.za/resource-center/threats/how-safe-is-your-smart-home

Samsung. (2019). Samsung Developers. Retrieved from https://developer.samsung.com/tv

Samsung. (2023). SmartThings. Retrieved from https://www.samsung.com/za/apps/smartthings/

Sovacool, B. K., & Furszyfer Del Rio, D. D. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews, 120*, 109663. doi:https://doi.org/10.1016/j.rser.2019.109663

Vogel. (2022). Smart Home Privacy: What Data Gets Collected, and What Can You Do About It? Retrieved from https://www.vogelme.com/post/smart-home-privacy-what-data-gets-collected