Attacks on and Defences of IoT Components in Smart Homes

Matthias Grabner
Freie Universität Berlin
14195 Berlin, Germany
m.grabner@fu-berlin.de

***Abstract*—IoT devices in smart homes have experienced a boom in the last few years, but the security landscape remains challenging. In this paper, the defining characteristics of IoT are presented, as well as their implications for security. Different methods of attacks are analysed and categorized using the five layer IoT architecture model. Their executability is rated, and it is assumed that the target is an average end-consumer of a Smart Home System. The effects of various security countermeasures are discussed in the context of the potential damage that successful attacks can have and the thereby resulting danger for consumers. Finally, an outlook on expected future developments and security considerations in IoT is given.**

***Index Terms*—IoT, Smart Home, Smart Home Systems, Security**

I. Introduction & Context

With the rampant adoption of the Internet of Things (IoT) in Smart Home Systems, the security of these devices has become increasingly important. Due to the intended functionality of these devices, a defining characteristic is their restricted physical resources, the diversity of data different devices handle and the heterogeneity of devices. These characteristics, along with other unique aspects that set IoT devices apart from traditional personal computers, necessitate a new and customized approach to security. With the Internet of Things being a relatively new phenomenon, security in this sector has not had a long time to mature.

With previous attacks, such as the Mirai Botnet DDOS attacks having demonstrated that users and companies who do not have any ties to the IoT industry, are also directly affected by IoT security, securing these novel devices is critical for the security of the whole internet.

Additionally, IoT devices are connected to the home networks of users, making them potential entry points for attackers. Even devices that cannot be exploited for uses beyond access to the network, can be used to infiltrate home networks. This interconnectedness poses significant, but inherent risks, as a compromised device can serve as a gateway to other devices and opens the network up to a plethora of other attacks, so-called internal attacks. However, many IoT devices are indeed vulnerable to various forms of direct exploitation that goes beyond accessing a network. These can range from simple disruptions to sophisticated intrusions aimed at stealing personal data or controlling the device remotely.

For the purpose of this paper, we will focus more on simple disruptions and attacks, as these often serve as the base for more complicated attacks. Additionally, a normal end-user is more likely to be the target of attacks that don't require a significant amount of effort per victim. An example of a more elaborate attack would be espionage using hardware Trojans in industrial or military contexts, or in fact most of the attacks concerning the physical layer. Instead, we will discuss and showcase methods of attacks that target end-consumers of IoT devices, along with safety precautions that can prevent these attacks or at least increase the effort required to execute them, thereby deterring attackers.

In section IV and VI we attempt to provide information that can help with the prioritization of different security improvements. This is done by analysing the potential types of damages that different types of attacks can have and attempting to categorize them by who is affected and by the severity with which these groups are affected. Additionally, the effort required to execute these attacks is discussed. For this, we will use users and external stakeholders to highlight areas where improvements in security are especially worthwhile. The paper will conclude with an outlook on future developments in IoT security in Smart Home Systems.

II. Security requirements

To arrive at a better understanding of security, this paper will use four characteristics that necessitate a new approach to their security, which we consider to be important, drawing on the work of Yang and Sun [1] and Sharma et al. [2]:

A. Characteristics of IoT

1) Large scale: With the rapid adoption of IoT devices, they are becoming more attractive targets for attackers, due to the increased amount of targets attackers can potentially target with one exploit. The increased size of IoT nets within single Smart Home Systems also leads to an increased attack surface and an increased amount of communication, producing new security issues as well as the need for scalable security solutions that can handle many devices at once [1].

2) Diversity: Diversity is present at many different levels in IoT devices, most importantly in the multimodality of data traffic and the varying granularity of data [1]. This means that data can take on different forms and arrive in different intervals of time and with different levels of detail. For example, speech recognition devices could send audio to analyse to a server every time the user uses it, while a fridge could send discrete

measurements every second. To account for this, security measures should ensure comprehensive protection across all types of data and traffic patterns.

3) Heterogeneity: A Smart Home System is the product of various different device types and families that use different protocols, hardware and algorithms [2]. This heterogeneity complicates securing the whole Smart Home System, as each type of device may have unique vulnerabilities and require different security measures. Standard protocols, interfaces and security concepts can help address these challenges by enabling better interoperability within the Smart Home System.

4) Physical constraints: IoT devices are designed with limited computing power, memory, and low energy consumption to fulfil their intended functionalities. These constraints severely limit the available countermeasures against attacks, as for example traditional authentication and key agreement (AKA) can't be used within most IoT devices [1]. Innovative security solutions tailored to the capabilities of IoT devices are necessary to protect them effectively.

B. Implications for Security

Each of these four features interacts with certain attack vectors and also provides a frame of attacks to be considered when designing a secure Smart Home System with IoT devices. These characteristics can inspire security enhancements both at the regulatory level and within individual IoT device manufacturers. For instance, implementing global interface standards that vendors must adhere to can address heterogeneity and its associated security challenges.

The features described above also limit the defence mechanisms that can be employed to fend off the range of possible attacks. Unlike traditional systems, IoT devices cannot implement the same security measures due to the physical constraints they are designed with. Therefore, securing both the individual devices and their communication within smart home systems is crucial. This includes ensuring the principle of data confidentiality, under which only friendly nodes should be communicated with by the existing network, new nodes have to authenticate themselves, and preventing the distribution of keys or data to attacker nodes. Additionally, maintaining data integrity and freshness, by making sure the data is not tampered with and also received without too much of a delay, is essential. Depending on the architecture, time synchronization also has to be executed securely to prevent synchronization attacks [2].

III. Methods of attack

Following a similar approach to Sharma et al. [2] we will use a layered architecture model to categorize security and attacks. Sharma et al. split the traditional network layer of the five layer model into a separate transport and network layer and omit the business layer [3]. However, we will be following the most common definition for discussing IoT in Smart Home Systems, seen in Fig. 1. In this model, each layer is responsible for different tasks that have to be secured respectively. For example, the network layer is responsible for "Routing, networking, topology management" [2]. As an example, this layer could be subject to flooding, replication and selective forwarding attacks, if an attacker could inject an enemy node into the network.

While other approaches, such as categorizing attacks into internal and external, exist, these transitions can be fluid and make an unequivocal classification challenging [2]. On the other hand, multiple layers can be affected by just one type of attack [1]. Other authors classify their own attack taxonomy, with Ho et al. only using three categories [4] and Heartfield et al. specifies 25 different types of attacks [5]. However, the most common and fitting definition for discussing IoT in Smart Home Systems seems to be the layered architecture model seen in Fig. 1.

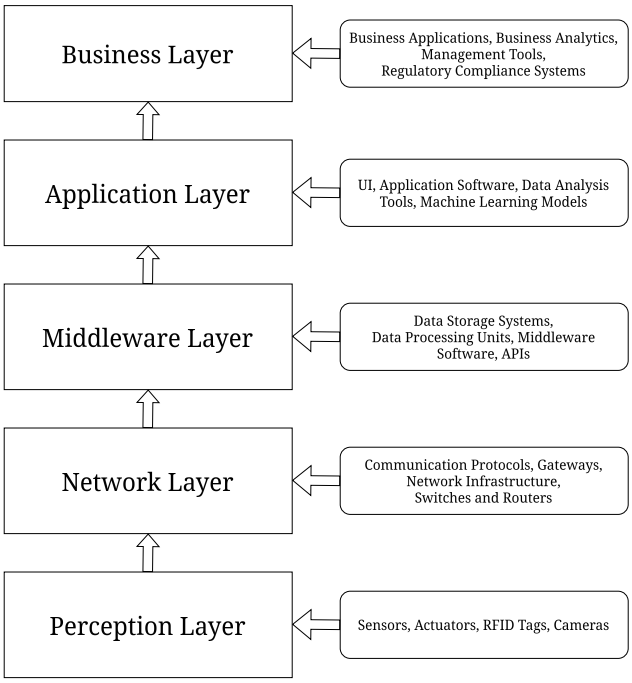

Fig. 1. Classic Layered IoT Architecture

A. Perception Layer

The perception layer (or physical layer) encompasses the hardware of the devices, as seen above in Fig. 1. Attacks targeting this layer include hardware Trojans [6], device tampering or jamming [2]. While Yang and Sun [1] lists hardware level threats as relatively rare in IoT devices in comparison to threats targeting other layers, Koley at al. [6] list them as a problem "growing day by day" and Karri et al. had already received a cover feature with an article about hardware trojans in the IEEE journal in 2010 [7]. The danger of attacks targeted at the physical layer can, be mostly attributed to hardware trojans and less so due to device tampering or jamming, as they require physical proximity to the target [6], especially in the context of Smart Home Systems. In specific, Koley at al. discuss the issue of integration density and the resulting

distributed manufacturing of integrated circuits [6]. Due to the many different vendors involved in the fabrication of a single IoT device and only one malicious circuit needing to be inserted to result in a hardware layer susceptible to attacks, a high-degree of security is difficult to achieve. Suggestions on how this could be attempted, will be summarized in section VI Additionally, Koley at al. also state that vulnerabilities can be injected in a chip after its manufacturing process by the actual IoT vendor [6]. Simple versions of these have the ability to modify outputs or leak information.

To emphasize the diversity of hardware Trojan threats, Karri et al. present a taxonomy for hardware trojans. Their proposed taxonomy lists the attributes of hardware Trojans as: insertion phase, abstraction level, activation mechanism, effects and location [7]. Karri et al. give examples for malicious modifications at each of the stages [7], including:

1) Changing the hardware's timing requirements
2) Using trojan infested standard cell libraries
3) Using different mask sets produced by wafers
4) Not trustworthy testing of integrated circuits
5) Assembling the integrated circuits in a way that introduce vulnerabilities

These stages, together with abstraction level, activation mechanism, effects and location, allow the authors to create a taxonomy for hardware Trojans that fulfil the self-imposed requirements of classifying all encountered and potential hardware Trojans in a resolution that allows researchers to distinguish trojans with "significantly different capabilities or required countermeasures" [7].

With these attributes being mostly independent of each other, a wide range of attacks and use-cases become thinkable. An example of an attack, using this taxonomy, would be an insertion at the register-transfer level by the company contracted to design the memory of the IoT device. This could achieve a memory-leak vulnerability in the final product, that could be exploited or sold to the highest bidder.

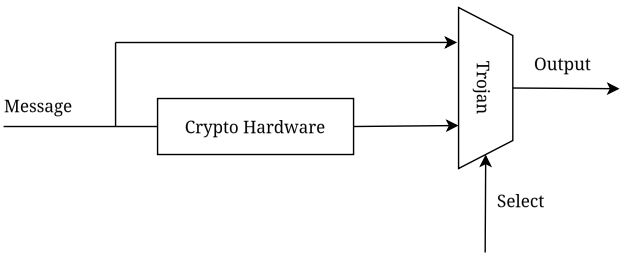

Fig. 2. Simple hardware Trojan, adapted from [7]

In Fig. 2 a visual example of a simple hardware Trojan is given. This Trojan is configured to send encrypted data, but allow external activation (select) to send unencrypted data. While this diagram shows the same output channel, duplicating the signal to be sent to a location specified by attackers is also possible to enable the unauthorized acquisition of confidential data.

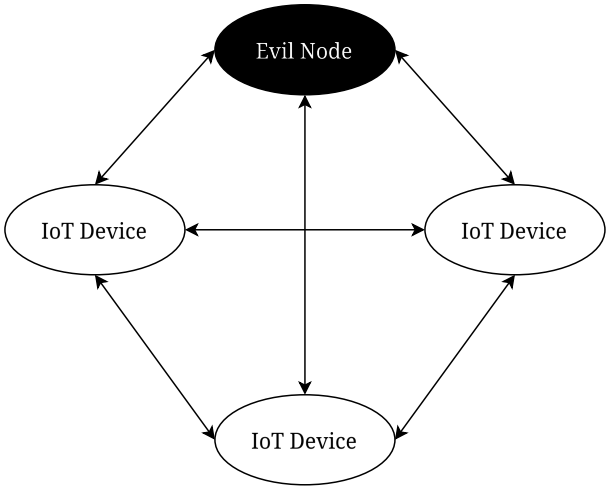

Fig. 3. Peer-to-Peer IoT Architecture

B. Network Layer

The network layer encompasses the transmission of data, as well as the protocols used for the transmission. The attacks targeting this layer are broad and complex, covering many different strategies and goals of attackers, explained in more detail in section V. Depending on how the IoT devices are connected to the internet and what specific architecture is used, the effectiveness and applicability of attacks vary widely. For example, a Smart Home System with a centralized architecture as seen in Fig. 4, where clients only communicate with one central server is not susceptible to black hole, selective forwarding and sinkhole attacks. This is due to the IoT devices possibly not having a routing function within centralized systems. In these attacks, an "evil" node chooses to modify the routing of packets, dropping all or some in black hole and selective forwarding attacks and advises false routing information in sinkhole attacks, as seem in Fig. 3. With no node-to-node communication, evil nodes cannot influence the routing of other nodes, without also compromising the central server.

However, other network attacks are not dependent on the architecture used. In hello flood attacks, for example, the infected node sends "Hello" packets to other nodes or the central server in a very short interval. With enough packets and no safety precautions, this causes a significant end-to-end delay, which increases with multiple infected nodes [2]. Another example would be energy drain attacks, in which messages are modified to increase the energy usage of some components, e.g a central server that is not allowed to go into standby mode or peer-to-peer nodes are subjected to unnecessary communication. Other attacks, which require physical proximity to the target, are mostly not applicable for end-consumers in the context of Smart Home System security.

Another important attack vector on the network level, mostly independent of the architecture used, are the protocols used for the transmission of data. Due to the characteristics of

IoT outlined in section II, the need for new and specialized protocols arises that cater to these. For example, NB-IoT tries to save power by only checking a narrow range of frequencies for updates [8], while MATTER tries to combat the heterogeneity of protocols and enable efficient communication between devices using different protocols [1]. All popular protocols used in IoT devices for Smart Home Systems, discussed by Yang and Sun, have been shown to face security issues of varying severity [1]. These include: LoRaWAN, BACnet, NB-IoT, 6LoWPAN and MATTER.

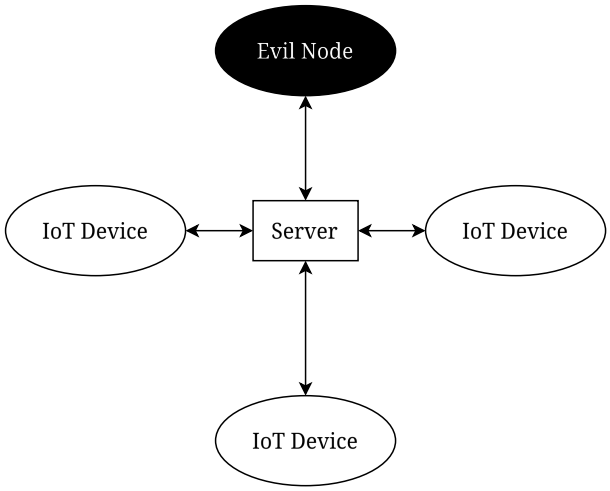

Fig. 4. Centralized IoT Architecture

C. Middleware & Application Layer

The middleware layer's task is mostly enabling the application layer to fulfil its functional requirements, for example by: "aggregating and filtering the received data from the hardware devices" [9]. Examples of components within this layer are data storage systems or data processing units. The application layer on the other hand includes: UI, application software and data analysis tools. In our analysis these layers are combined, as most IoT devices do not offer the installation of proprietary software to the user, which would result in different attack vectors for the two. In such scenarios, protection mechanisms should be put in place to verify that user-installed software does indeed have non-malicious intents. However, with manufacturers mostly providing both the middleware and the application layer, the methods of attack are mostly similar, rendering a distinction useless for the purpose of this paper.

A persistent issue is the lack of updates both of these layers receive from the manufacturers, even after vulnerabilities become known, leading to devices potentially becoming unsecure fast. Koley et al. list this problem as one of the five key challenges of IoT security [6].

Attacks targeting this layer are mostly malicious code attacks, and Sharma et al. also lists path-based DoS attacks and attacks on reliability [2]. Path-based DOS attacks are an advanced type of denial-of-service attacks, only targeting specific paths in the network, making them unusable for regular traffic. This can affect data integrity, as sensor readings can't be communicated any more or expose security vulnerabilities or any number of issues arising from the inability to communicate with other devices in the network.

Additionally, attacks focused on compromising the security of the device by attempting to log in through the same interface as the user could be considered to fall under this layer. This is attempted in brute-force attacks, default password attacks, or attacks where the user credentials were obtained through other means.

D. Business Layer

The IoT system is managed by the business layer [3]. This layer defines the integration, management, and optimization of technologies and systems to support the IoT vendor's objectives. This layer includes, among many other things: API management, interoperability, cloud services and infrastructure.

However, as most of the things included in this layer are not IoT specific, similar to existing analyses, it will not be discussed further in this section. Still, the business layer opens up the possibility to offload some of the calculation intense tasks of security countermeasures [1], eliminating one of the key characteristics of IoT systems discussed in section II, which will be discussed in section VI.

IV. Executability and Effort

This section can be split into two basic subsections: hardware and software based attacks, as the layers presented in section III do not necessarily correlate with either executability or effort, apart from their division in hardware and software based attacks.

A. Hardware

As explained briefly in subsection III-A, hardware attacks can be executed by any contracted company in the design and manufacturing process. For these companies or individuals within these companies, the effort to execute such an attack is relatively low effort, as it just a slight variation of their usual job. While not directly IoT related, previous publicized cases of poor supply chain security and the resulting failures in hardware, include counterfeit routers being used in US defence and finance networks [7].

For end-users who are usually not specifically targeted by attackers, but only as a group, the fact that hardware Trojans are almost impossible to target individuals with, does not play a role. Instead, attackers may be encouraged by the prospect of targeting all users of a specific device at once with a relatively low amount of effort. This results in the fact that depending on the regulation in the countries of manufacture and the awareness of the IoT device vendor, hardware Trojans and other hardware security compromising counterfeits represent a realistic scenario. As Karri et al. state: "For reasons of economy, critical systems will inevitably depend on electronics made in untrusted factories" [7]. For end-consumers, who

may look for the cheapest IoT devices on the market, this is even more true. With no standard, agreed-upon way of labelling security features and informing customers of the risks associated with buying certain low-priced devices, consumer awareness about this topic can also not be expected.

B. Software

Without physical access, most attacks rely on either on social engineering, unpatched vulnerabilities or an already infected IoT device, which would then constitute a so-called internal attack [1]. Exploiting unpatched vulnerabilities or poor security practices can cover the whole spectrum of easy to execute to extremely hard to execute, depending on how severe and critical the vulnerability is. For example, the infamous Mirai Botnet with a few hundred thousand infections was created using the default credentials of many devices and attempting to log in, before downloading its malware and propagating further. Compared to the potentially extremely high material gain of the attackers, in this case, the effort required was very low (apart from the fact that the malware's were customized and adapted to many different architectures of their targets) [10].

The executability and methods of attack also depend on how many of the Smart Home Systems layers are exposed to long-range attackers. This is highlighted in Fig. 5, where the upper node communicates via a low-range protocol (in this case ZigBee) and the lower node operates with a long-range protocol, such as HTTP. Communicating via a low-range protocol or making sure the device can only be accessed from inside the network, would drastically reduce the points of attack, as the devices apart from the central server could not be subjected to many remote, direct attacks. If the functionality to address these secondary nodes by remote protocols is disabled, the network layer is no longer exposed.

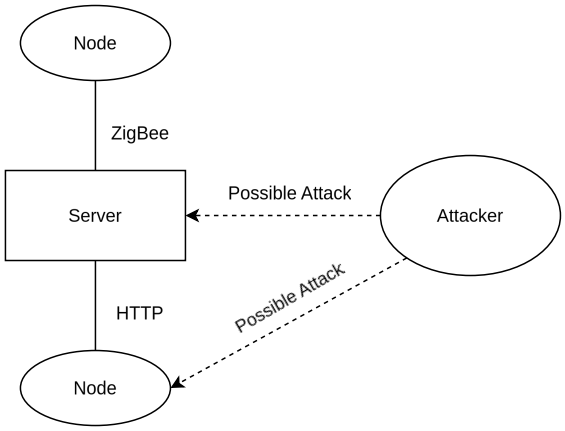

Fig. 5. Possible Remote Network Layer Attacks

However, once one IoT device in a network has been compromised, various internal attacks can be started against other parts of the Smart Home System. These internal attacks use knowledge or access that attackers should not possess to their advantage. As low-range protocols are not without their fair share of vulnerabilities, previously security-positive measures may now result in an easier attack of other components [11].

An example of another internal attack, possible with many protocols, would be the "Evil Node" scenario outlined in section III-B. For this category of attacks, any previously "hidden" layers can be attacked again using the privileged access to the network.

V. Potential for Damage

A. Types of Damages

Different groups and individuals are affected by the results of the attacks explained above. These can be categorized roughly into the affected user themselves, the general internet-using public and individual companies.

1) The User: Users can be affected in a variety of ways by malicious attacks. Damages can be financial (energy attacks), loss of privacy which can occur in many different attacks, or a disruption in the functioning of the IoT devices or the home network of the user [1].

2) The Public: As seen in the Mirai Botnet attacks, the general public can be affected by insecure IoT devices as well. In this case, the attack on the DNS provider DYN caused many popular websites such as Amazon, Netflix and Twitter to be inaccessible to many users [10].

3) Individual Companies: The Mirai Botnet did not only attack DYN, but also individual companies such as Lonestar. Lonestar specifically was attacked due to a rival company paying the author of a Mirai variant to take them down [12]. However, also Hardware Trojans can be used to target the customers of individual companies and harm their reputation [7].

B. Damages of Attacks

The damages of known IoT related attacks vary widely and can also not be quantified easily. However, the traditional facets of security: Confidentiality, Integrity, Availability, and Accountability can be examined. Neshenko et al. suggest that each category can be relatively easily attacked and compromised. For example, device-based vulnerabilities such as insufficient energy harvesting or bad physical security can lead to integrity and availability being impacted [13]. The insufficient energy harvesting can be exploited by attackers by using various methods to drain the stored energy in the device, impacting availability.

VI. Safety Precautions

A. Hardware Trojans

Due to their diverse nature, defending devices against hardware Trojans proves to be an extremely difficult task. The field of Hardware Trust, among other things, focuses on how to achieve this task. Some areas of research and utilized methods in the industry of integrated circuits include: design for test, tamper resistance, logic verification and side channels [7]. However, most of these prove to be ineffective against hardware Trojans. For example, design for test enables the verification of hardware to ensure that it works just as

intended, but usually only tests for naturally occurring faults. This is an issue, as "a system can pass a set of tests that has 100 percent coverage for naturally occurring faults but can still contain a hardware Trojan" [7]. Similarly, tamper resistance can only effectively increase the cost to attackers, but also scales for the designing and producing company and may introduce new complexity, having a negative impact on non-functional requirements of the integrated circuit [14]. Logic verification does not protect against Trojan insertions at the specification or fabrication phase [7]. The listed factors, together with the economic factors discussed in section III-A make it currently almost impossible to defend against this type of attack, especially for consumers.

To restrain the effect of these economic factors, the most effective approach in our opinion would be forcing the traceability of components and discovered hardware Trojans through legislature. Additionally, mandatory certifications for companies and a vetting process for employees handling what is about to be part of a critical infrastructure could be introduced. If this is introduced, an introduction along the whole design and production process would be vital, as the injection of a Trojan can take place in any phase of development [7].

B. Network Attacks

As already mentioned in section III-B, a centralized "hub" can help to reduce the effect of one infected node on the network and on other IoT nodes. Such a centralized structure can also be beneficial due to the availability of efficient low range protocols, specifically designed for IoT. By only communicating with a central hub that is able to forego many of the presented inherent restrictions of IoT devices, the individual IoT devices become practically invisible to the outside world beyond the range of the low range protocols [8]. Such a smart home hub is also only needed once per home, meaning that the household can encompass just three or even twenty IoT devices and centralize them with just one hub. For consumers, this can present a significant security improvement, as they are usually not attacked with the attacker being in physical proximity.

The most popular protocols also presented in section III-B, seem to be similar in terms of the level of security they can provide the user with. While they all have significant security weaknesses, they are not inherently securer than one another, which could justify the recommendation of a specific protocol.

C. Middleware & Application Layer

Improving the security of the middleware and application layer boils down to improving the general security practices within the companies creating new IoT devices. Standard passwords and no updates even for recently released devices account for many successful intrusions into IoT systems [10] [6]. Otherwise, the standard solutions and quality assurance processes implemented to create secure software for conventional devices, should also be applicable to the domain of software for IoT device.

D. Cloud Computing

As mentioned in section III-D, cloud computing can partially alleviate the inherent resource restriction of IoT devices. By doing so, it becomes a valuable measure in securing attack-vectors that only exist due to a lack of local computational power. However, introducing connections to an external cloud and implementing them increases the complexity of the Smart Home System and results in many new security challenges including: "remote authentication, secure data exchange and collaborative control" [1]. The necessity of introducing these new challenges and the risk to usefulness ratio is therefor dependent on the specific use case and should be carefully considered.

E. Cost and Consumer choice vs security dichotomy

Unfortunately, all the safety precautions presented above result in a more expensive product. Higher standards for supply chains would increase the price of the product [7], a central IoT hub (assuming it is compatible with all owned devices) is a significant cost factor and effectively renting cloud computing power presents an ongoing cost factor. This presents quite a difficult choice for consumers, who are able to choose between cheaper and more expensive, but also more secure smart home solutions. However, security doesn't seem to be a priority (at least when compared to ease of use) for many users as shown by Grobelna et al. [15]

VII. Outlook and Conclusion

A. Future outlook on security developments

The current state of IoT security does not seem to be advanced in comparison to the widespread use of IoT devices. As Yang and Sun state: "the research on security issues in SHSs is far behind the speed of SHS development" [1]. More research is required to solidify the current findings, and create solutions to current problems. Yang and Sun categorize them as: a unified Smart Home System architecture, security in low-performance devices, fragmentation and firmware security analysis [1].

B. Recommended security improvements

Until the listed areas of research have been more thoroughly investigated, vendors can implement relatively easy and effective security improvements that have been known to work for a long time, but just weren't implemented. In fact, the security of consumer-level IoT devices is not up-to-date with even general security practices [16]. Theoretical knowledge of the safest possible way to achieve the desired functionality can only go so far, if it isn't even being considered by vendors who refuse to implement basic safeguards against attacks.

1) No Default Passwords:: As the Mirai botnet has shown, many vendors (at least at the time of the attack in 2016) use default passwords. In 2023, default passwords were still widespread, according to an analysis done by van Harten et al. [16].

2) Automatic Updates: : Even though this measure is very easy to implement, 13 of 40 consumer-level IoT devices analyzed by van Harten et al. only offer manual updates [16]. In this case, implementing this security practice would also enhance user-comfort. Often, security measures are seen as having a negative effect on user comfort, which isn't the case here.

3) Information Material: : This measure is aimed at informing the user about the risks of certain security practices and helping users to make an informed decision. Information material only works indirectly, as it encourages other practices that do then improve the security of Smart Home Systems. When compared to the governmental advice given by the UK, the US and the Netherlands, no device in a sample of 40 provides information on the four categories of: default credentials, router, updates and network connectivity [16].

C. Conclusion and Recap

In this paper, we have outlined the need for a distinct view of security for IoT devices based on the common characteristics of IoT devices in smart homes. The five layer model for IoT devices (perception, network, middleware, application and business layer) was used to classify and summarize exemplary attacks such as the hardware Trojan seen in 2. The influence of architectural decisions on security was discussed in section III-B. Middleware and Application layer were combined, and the business layer was omitted. The ease with which these attacks can be executed was roughly discussed, using the much wider granularity of hardware and software. Next, the damage potential of these attacks was shortly analyzed, differentiating between the affected groups. Lastly, exemplary safety precautions presented in the reviewed literature were presented.

REFERENCES

[1] J. Yang and L. Sun, "A Comprehensive Survey of Security Issues of Smart Home System: "Spear" and "Shields," Theory and Practice," *IEEE Access*, vol. 10, pp. 124167–124192, 2022.

[2] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues," *Electronics*, vol. 10, p. 2365, Jan. 2021. Number: 19 Publisher: Multidisciplinary Digital Publishing Institute.

[3] M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "IoT Architecture," in *Towards the Internet of Things: Architectures, Security, and Applications* (M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, eds.), pp. 9–31, Cham: Springer International Publishing, 2020.

[4] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart Locks: Lessons for Securing Commodity Internet of Things Devices," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, (New York, NY, USA), pp. 461–472, Association for Computing Machinery, May 2016.

[5] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. J. Fontaine, A. Filippoupolitis, and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," *Computers & Security*, vol. 78, pp. 398–428, Sept. 2018.

[6] S. Koley and P. Ghosal, "Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions," in *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, pp. 517–520, Aug. 2015.

[7] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," *Computer*, vol. 43, pp. 39–46, Oct. 2010. Conference Name: Computer.

[8] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*, vol. 3, pp. 14–21, Mar. 2017.

[9] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A General Overview between Architectures, Protocols and Applications," *Information*, vol. 12, p. 87, Feb. 2021. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[10] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, (Vancouver, BC), pp. 1093–1110, USENIX Association, Aug. 2017.

[11] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[12] "Inside the infamous Mirai IoT Botnet: A Retrospective Analysis," Dec. 2017.

[13] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019. Conference Name: IEEE Communications Surveys & Tutorials.

[14] R. Anderson and M. Kuhn, "Tamper resistance-a cautionary note," in *Proceedings of the second Usenix workshop on electronic commerce*, vol. 2, pp. 1–11, 1996.

[15] I. Grobelna, M. Grobelny, and G. Bazydło, "User awareness in IoT security. A survey of Polish users," *AIP Conference Proceedings*, vol. 2040, p. 080002, Nov. 2018.

[16] V. van Harten, C. H. Gañán, M. van Eeten, and S. Parkin, "Easier said than done: The failure of top-level cybersecurity advice for consumer iot devices," 2023.