IoT Security: A Basic IoT Hardware Security Framework

Christoph Haar
Hochschule für Telekommunikation Leipzig
Leipzig, Germany
Email: haar@hft-leipzig.de

Erik Buchmann
Leipzig University
Leipzig, Germany
Email: buchmann@informatik.uni-leipzig.de

***Abstract*—More and more Internet of Things (IoT) devices are being used in companies today. The usage harbors great risks, because numerous observations have shown that many IoT devices on the market are insecure. For this reason, well-known security authorities such as the German Federal Office for Information Security (BSI) or the National Institute for Standards and Technologies (NIST) have established standards and guidelines, considering known threats and common security practices for IoT devices. They focus on software security as well as the secure planning and usage of IoT devices. Hardware security on the other hand is less considered. In this paper, we develop a basic IoT hardware security framework that can be implemented into existing security concepts. To reach this goal, we compare three official IoT security standards to identify important hardware threats. After that, we perform a risk identification for four different IoT devices to find out if the mentioned hardware threats really apply to different application scenarios. Based on the results, we develop a basic IoT hardware security framework. Our research has shown that the hardware threats mentioned in the official IoT security standards are of great importance. Because they apply to a wide range of different application scenarios for IoT devices, we implemented them in our basic IoT hardware security framework.**

Keywords – IoT Security Standards, IoT Hardware Threats, Risk Identification, Security Framework.

I. INTRODUCTION

Over the last years, the number of connected IoT devices in enterprises has increased rapidly [1]. They are used to improve the productivity of business processes or to massively reduce costs [2] [3]. On the other hand, there are numerous threats associated with their use [4]–[7]. Observations have shown that many IoT devices on the market are insecure [8]. Attackers can compromise them, spy out internal data and interrupt services. The damage caused by such attacks can be existence-threatening. Official security authorities, such as the German Federal Office for Information Security (BSI), the National Institute for Standards and Technology (NIST) or the European Union Agency for Cybersecurity (ENISA) have already addressed this issue. Numerous free IoT security standards also have been published during the last years. They consider known threats and common security practices. A closer examination reveals that there is no uniform process for IoT hardware security. The hardware is the basis of any IoT device [9]. Thus, there should be a structured process for basic protection. The aim of this paper is to develop a basic IoT hardware security framework that can be used to protect any IoT device on a basic level. For this purpose, we compare three official IoT security standards, published by BSI, NIST and ENISA to identify important IoT hardware threats mentioned in the standards. The result of this comparison serves as the basis for a risk identification. We select four different and commonly used IoT devices and perform a risk identification to be able to find out if the mentioned hardware threats really apply to different application scenarios. Based on the results, we derive a basic IoT hardware security framework that includes the identified risks. Our basic IoT hardware security framework consists of three steps. Following these steps ensures a basic protection of any IoT device regardless of its application scenario.

Paper structure: Section II contains the related work. In Section III, we perform a risk identification and generalize our findings. In Section IV, we define the IoT hardware security framework, followed by a discussion in Section V. Section VI concludes the paper.

II. RELATED WORK

In this section, we introduce three official IoT security standards and compare, which hardware threats are mentioned. In this way, we are able to identify particularly important threats. At the end of this section, we give a brief introduction into risk identification.

A. IoT Hardware Security

The security of IoT devices should start with the security of the hardware because it is the basis of any device [9]. There are already numerous publications, describing hardware threats and suitable security practices for IoT devices [9]–[13]. Also official security standards have been developed and published to ensure a secure usage of IoT devices and all their data, as well as the entire system on which they are operated. Each standard considers hardware security differently.

a) BSI: The BSI describes 47 product and technology-neutral elementary threats in the BSI standard 200-3 [14]. They describe general risks for IT systems, regardless of their application scenario. Not every elementary threat is affecting each part of an IT system. The BSI lists all elementary threats that are addressing a certain element of the IT system in the

IT Grundschutz Compendium [15]. For example, the module ”‘SYS.4.4 General IoT Devices”’ contains an appendix which considers 20 of the 47 elementary threats that are affecting IoT devices as Table I illustrates.

TABLE I
IoT Elementary Threats

BSI Elementary Threats For IoT Devices
G 0.2 Bad Environmental Conditions
G 0.4 Pollution, Dust, Corrosion
G 0.8 Disruption of Power Supply
G 0.9 Failure or Disruption of Communication...
G 0.14 Interception of Information / Espionage
G 0.16 Theft of Devices, Storage Media and...
G 0.18 Poor Planning or Lack of Adaptation
G 0.19 Disclosure of Sensitive Information
G 0.20 Information or Products from an...
G 0.21 Manipulation with Hardware
G 0.23 Access to IT Systems
G 0.24 Destruction of Devices or Storage Media
G 0.25 Failure of Devices or Systems
G 0.26 Malfunction of Devices or Systems
G 0.28 Software Vulnerabilities or Errors
G 0.29 Violation of Laws or Regulations
G 0.30 Unauthorised Use or Administration of...
G 0.38 Misuse of Personal Information
G 0.39 Malware
G 0.40 Denial of Service

These threats apply to all IoT devices regardless of their application scenario or security properties. They consider the hardware and software, as well as a secure planning and usage. Because they are completely unsorted, it is up to the user to identify the hardware related threats.

b) NIST: The *National Institute for Standards and Technology (NIST)* published several drafts for IoT security in 2020 [16]–[20]. They consider the acquisition and implementation of IoT devices in companies and give an overview about important steps that need to be considered, when planning to use IoT devices. They also describe how the data of IoT devices can be protected, as well as the entire system. As Table II illustrates, the NIST does not use elementary threats like the BSI but similar hardware threats are mentioned.

TABLE II
NIST IoT Hardware Threats

NIST Hardware Threats For IoT Devices
Physical Damage
Unauthorized Access
Hardware Manipulation

The NIST specifies the mentioned threats. Physical damage includes vandalism, as well as damage through high or low temperatures and humidity [16]. This is similar to G 0.2 Bad Environmental Conditions and G 0.24 Destruction of Devices or Storage Media. It is also mentioned that IoT devices may have to endure physical damage through extreme temperatures that could be caused by a fire. Unauthorized Access is considered by considering the restriction of network and local interfaces [17]. That means, the IoT device must be able to deactivate local and network interfaces. In this way, open communication interfaces could be deactivated to avoid unauthorized access. This covers the elementary threat G 0.23. Hardware manipulation is addressed by mentioning the use of unique physical identifiers [17]. There is no precise definition of what is meant by unique physical identifier, but there are approaches, such as PUFs that leads to an unique behavior of the device. Any physical manipulation would change this unique behavior and detect the manipulation. This is similar to G 0.21 Manipulation of Hardware.

The hardware threats are mentioned in different sections of the drafts but there is no separate section or even a clear process that defines general steps for protecting the hardware.

c) ENISA: The *European Union Agency for Network and Information Security* (ENISA) [21] published the Baseline Security Recommendations for IoT. This publication contains a hardware security section. It is addressing IoT security challenges and provides general security recommendations when using IoT devices. Many hardware threats are considered as shown in Table III.

TABLE III
ENISA IoT Hardware Threats

ENISA Hardware Threats For IoT Devices
Elemental Threats
Environmental Threats
Physical Damage
Hardware Manipulation
Power Loss
Data Interception

The mentioned threats are also similar the elementary threats from the BSI. ENISA separates the threat physical damage. It is only caused through vandalism. Threats like water and fire are not considered as physical damage but as elemental threats. Environmental threats on the other hand are causing damage through high or low temperatures. Interception is not only a physical threat. It is mentioned that all kinds of data interception has to be considered. That could be the interception of data traffic or stored data but also the interception of electromagnetic radiation emitted by the hardware. Also the usage of hardware that provides security features like specialised security chips to detect physical manipulations is recommended. Disruption of power supply is another mentioned threat. Even though ENISA has introduced a separate section for hardware security, there is still no clearly defined process for hardware protection.

It can be clearly seen that the mentioned hardware threats are very similar in the three security standards. Sometimes the threats are just categorized differently. For example the NIST considers fire as physical damage. For ENISA, on the other hand, it is an elementary threat. However, both standards consider fire as a threat.

Since the hardware threats are so similar in the individual standards, we use the 47 BSI elementary threats as a basis for our risk identification. The elementary threats are also product and technology-neutral and compatible with other international catalogs and standards.

B. Risk Analysis

In 2017, the BSI published the current version of the BSI-Standard 200-3 [14] that defines the steps of a risk analysis. The first step is the risk identification. Threats that are realistic for a certain target object and its application environment are identified by IT-security experts in a brainstorming session. IT-security experts means information security officers, responsible specialists, administrators, users of the target object and if available external expert. The risk identification is a very important step, because not identified threats will lead to a major security gap. It is only possible to classify threats and define appropriate security practices for identified threats. ENISA also starts the risk analysis process by considering security incidents that have become public over the last years. Also a threat taxonomy is illustrated [21]. Other official security authorities like NIST [22] also define a risk management process that starts with a risk identification.

They all understand risk identification as a fundamental step for further risk management activities.

III. RISK IDENTIFICATION

In this section, we perform a risk identification for the hardware of four different IoT devices. In the first step, we select four IoT devices and list all their hardware components. We use the hardware components to determine, which hardware threats are affecting the IoT device. After that, we analyze the 47 elementary threats from the BSI and select those that potentially address the hardware. This is necessary because the elementary threats from the BSI are not limited to the hardware. In the next step, we perform the risk identification. In particular, we systematically analyze for each IoT device which hardware components are affected by the potential hardware threats. Finally, we analyze and generalize our findings.

A. IoT Devices

For our investigation, we select four commonly used IoT devices. The IoT Security Camera [23], the IoT Smoke Detector [24], the IoT Soil Temperature Sensor [25] and the IoT Power Outlet [26]. The application scenarios of the devices are as different as possible. In this way, we are able to determine if the mentioned IoT hardware threats from the BSI really apply to a wide range of different application scenarios.

Table IV gives a brief overview of all hardware components of each IoT device.

TABLE IV
IoT Device Hardware Components

Security Camera	Smoke Detector
Cables, Camera, Case, Infrared LED's, Micro SD socket, Microphone, Motherboard, Processor, Sensors	Battery, Case, LED, Motherboard, Processor, Reset Button, Sensors, Speaker
Soil Temp. Sensor	**Power Outlet**
Antenna, Battery, Case, Motherboard, processor, Sensors	Case, Motherboard, Processor, Sensors, Socket Connector

B. Potential IoT Hardware Threats

The elementary threats, defined by the BSI cover a wide range of potential threats for an entire company. They also consider many hardware threats. We do not consider all of them in this paper. Table V summarizes the hardware threats we consider. We consider damage caused by G 0.1 Fire, G 0.2 Bad Environmental Conditions and G 0.3 Water because these threats are always conceivable. For example, Water damage can be caused by simple rain. Fire can be caused by a short circuit and bad environmental conditions can stem from to high or low temperatures. We also consider that an IoT device can be damaged by excessive pollution. Dust and soil can intrude through leaks and damage hardware components. This threat is considered in G 0.4 Soiling, Dust, Corrosion.

TABLE V
Potential IoT Hardware Threats

Potential IoT Hardware Threat
G 0.1 Fire
G 0.2 Bad Environmental Conditions
G 0.3 Water
G 0.4 Soiling, Dust, Corrosion
G 0.8 Disruption of Power Supply
G 0.12 Electromagnetic Interference
G 0.13 Interception of Radiation
G 0.21 Manipulation of Hardware
G 0.23 Unauthorized Entry
G 0.24 Destruction

On the other hand, we do not consider G 0.5 Natural Catastrophes, G 0.6 Catastrophes in the Environment and G 0.34 Attack. These threats do affect the entire hardware but they are extreme events. Normally, IoT devices cannot be protected against such incidents. G 0.8 Disruption of Power Supply considers service interruptions or physical damages caused by a sudden power loss. The reason for this could be a storm that could occur at any time. Thus, we do also consider this threat. The BSI also mentions G 0.12 Electromagnetic Interferences as an elementary threat. Although it is not mentioned as an elementary threat to IoT devices, the BSI points out that all electronic devices are affected by G 0.12. Furthermore, the BSI emphasizes that also wireless communication like WI-FI can be affected by electromagnetic interferences. Because IoT devices are electronic devices and they do communicate wireless, we consider this threat. Data can be revealed through electromagnetic interferences. The BSI is mentioning this threat in G 0.13 but does not consider it as an elementary threat for IoT devices. ENISA on the other hand mentions that all threats that intentionally or unintentionally reveal data has to be considered. Due to this fact, we also consider G 0.13 Interception of Radiation. This could also be considered as G 0.14 espionage but this security practice also includes non hardware aspects like the interception of data traffic. Due to this fact, we do not consider G 0.14 espionage. We do also not consider G 0.16 Theft of Devices, because the hardware is not necessarily affected by a theft. G 0.21 Manipulation of Hardware means every willful change of the original hardware that leads to an unnoticed change in behavior. Since devices are usually purchased from unknown manufacturers, manipulation of the hardware cannot be ruled out. Thus, we also consider this threat. With G 0.23 Unauthorized Entry, the BSI considers physical access via unprotected communication interfaces like USB ports [11]. Because many IoT devices have such open communication interfaces, we also consider this threat. The BSI differentiates between G 0.41 Sabotage and G 0.24 Destruction. In both cases the aim is to damage the IT systems. Destruction means willful attacks against the device by impact. Sabotage describes the manipulation of the environment that leads to a damage of the IT system. For example closing the ventilation slots of a server, which leads to overheating and finally damage or destroy the server. Since both threats have the same goal, we summarize and consider them in G 0.24 Destruction.

C. Implementation

In this step, we implement the risk identification. That means, we analyze which hardware components are affected by the potential hardware threats. Furthermore, we check for each of the four IoT devices whether it has the affected hardware component. **G 0.1 Fire** A fire cannot be assigned to a specific hardware component. It could lead to a damage of all hardware components of any IoT device. Therefore, we consider all four IoT devices as affected.

G 02. Bad Environmental Conditions All four devices have a clear defined operating temperature. That makes their entire hardware affected by G 0.2 Bad Environmental Conditions. The security camera can be operated between -10 and +55 degrees. The smoke detector and the power outlet on the other hand can only be operated above 0 degrees up to +40 degrees. The soil temperature sensor has the largest operating temperature range from -40 to +80 degrees. If the devices are operated outside the specified operating temperature, all hardware components could be damaged. Thus, we consider all four devices as affected.

G 03. Water In case of a water intrusion, non electric components would not be affected. For example, all four devices have a plastic case. This case can be wet but it would not be damaged by the water. The damage would caused to electronic components. All four devices have electronic components like sensors, processors or LEDs. Thus, we consider all as affected.

G 0.4 Soiling, Dust, Corrosion Like G 0.3, this threat does not affect non electric components like the plastic case or buttons. Soiling, dust and corrosion would only cause damage to electronic components. For example the sensors of all four IoT devices could be disturbed by to much pollution or the processor could overheat. Furthermore, the electronic components could rust after moisture has entered the device. Because all four devices have electronic components, we consider all as affected.

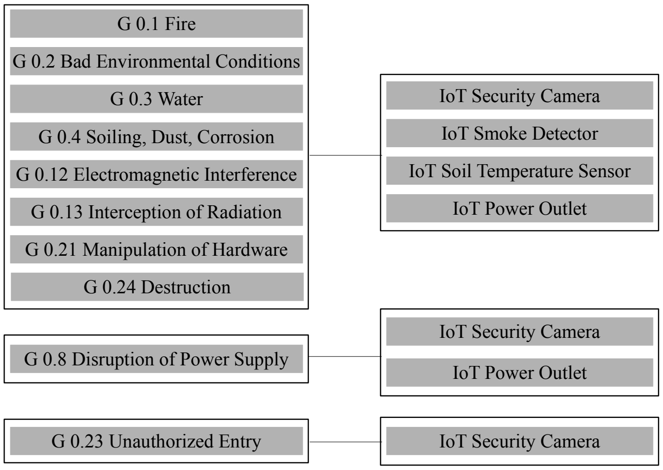
G 0.1 Fire
G 0.2 Bad Environmental Conditions
G 0.3 Water
G 0.4 Soiling, Dust, Corrosion
G 0.12 Electromagnetic Interference
G 0.13 Interception of Radiation
G 0.21 Manipulation of Hardware
G 0.24 Destruction
IoT Security Camera
IoT Smoke Detector
IoT Soil Temperature Sensor
IoT Power Outlet
G 0.8 Disruption of Power Supply
IoT Security Camera
IoT Power Outlet
G 0.23 Unauthorized Entry
IoT Security Camera

Fig. 1. IoT Device Threats

G 0.8 Disruption of Power Supply The IoT security camera and the IoT power outlet have a power connection. These devices do not have batteries what makes them dependent from external power sources. As soon as the power supply is interrupted, both devices will be turned off immediately. Due to this fact, we consider them as affected. The IoT smoke detector and the IoT temperature sensor are battery operated. That means, they are not connected to power sources and therefore unaffected by this threat.

G 0.12 Electromagnetic Interference All electronic devices can be disturbed by electromagnetic interferences. That means, every electronic hardware component is affected. Since each of the four IoT devices is an electronic device, we consider them as affected.

G 0.13 Interception of Radiation All electronic devices emit radiation. That means, every electronic hardware component is affected. Since each of the four IoT devices is an electronic device, we consider them as affected.

G 0.21 Manipulation of Hardware Manipulation of hardware can also not be assigned to a specific hardware component. For example, the case of all 4 devices could be manipulated in such a way that water intrudes and cause damage. The sensors could also be manipulated so that incorrect measurement results are transmitted. Thus, we consider all hardware components of each device to be affected.

G 0.23 Unauthorized Entry The IoT security camera is the only device that has an open communication interface. It is possible to connect SD cards. An attacker could use this SD card socket to gain unauthorized access to the IoT security camera or the entire network. Due to this fact, we consider the IoT security camera as affected. The other three devices not have any open communication interfaces, thus we consider them as not affected.

G 0.24 Destruction It is always possible for an attacker to intentionally destroy any hardware component of each of the four devices. Thus, we consider all four devices as affected.

Figure 1 summarizes the results of our risk identification.

It can be seen that each of the four devices is addressed by at least one threat. G 0.23 is only affecting the IoT camera. This is because it is the only device with an open communication interface. G 0.8 Disruption of Power Supply is affecting the IoT camera and the IoT power outlet because they are connected to the buildings electricity. All other threats are affecting each of the four IoT devices. With our risk identification, we were able to confirm that the threats mentioned in the official IoT security standards apply to different application scenarios. In the next step, we generalize our results to be able to use them as a basis for our framework.

a) Generalization: As we can see, a hardware threat can only affect an IoT device, if it has the addressed hardware component. For example, G 0.23 Unauthorized Entry can only affect IoT devices that have open communication interfaces like USB ports. Figure 2 illustrates hardware components that are affected by the potential IoT hardware threats.

We were able to determine that G 0.1, G 0.2, G 0.21 and G 0.24 are affecting every hardware component. That means, as soon as a device exists, *all components* are addressed. G 0.3, G 0.4, G 0.12 and G 0.13 are affecting all *electronic components* in general. Since every IoT device communicates electronically, it also consists of electronic components. Due to this fact, all IoT devices are affected. G 0.8 is addressing *power connections* to the building's electricity. That means, battery operated devices are generally not affected. G 0.23 is affecting all IoT devices with *open communication interfaces.*

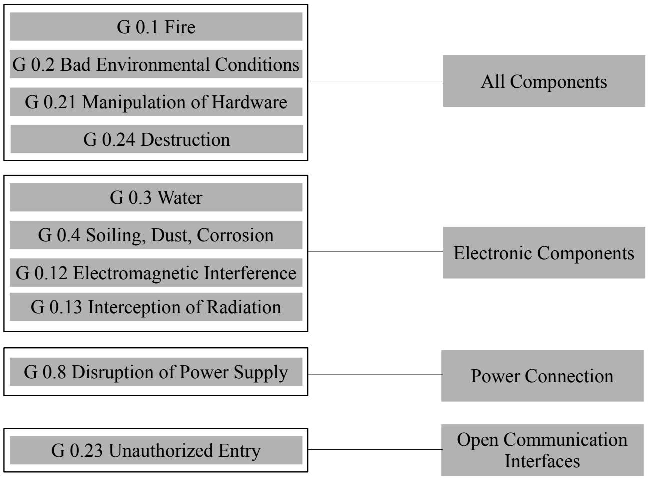
G 0.1 Fire
G 0.2 Bad Environmental Conditions
G 0.21 Manipulation of Hardware
G 0.24 Destruction
All Components
G 0.3 Water
G 0.4 Soiling, Dust, Corrosion
G 0.12 Electromagnetic Interference
G 0.13 Interception of Radiation
Electronic Components
G 0.8 Disruption of Power Supply
Power Connection
G 0.23 Unauthorized Entry
Open Communication Interfaces

Fig. 2. Affected Hardware Components

IV. FRAMEWORK DEFINITION

With our risk identification, we found out, which of the hardware threats mentioned in the official IoT security standards apply to different IoT devices. In this way, we were able to confirm that these threats are of particular importance for the hardware of IoT devices. These threats must either be considered for all IoT devices or at least for a large number of different application scenarios. Due to this fact, we define a basic IoT hardware security framework that considers these threats in this section. There is a total of four hardware threats (G 0.1, G 0.2, G 0.21 and G 0.24) that apply to all hardware components of each of the four IoT devices. Because they are also mentioned in the official IoT security standards, they should definitely be considered when securing IoT devices. Same holds for the four hardware threats (G 0.3, G 0.4, G 0.12 and G 0.13) that are affecting all electronic hardware components of each of the four IoT devices. Because every IoT device has electronic components, they should also definitely be considered. There are two hardware threats that only apply, in case the IoT device has a certain hardware component. G 0.8 is only affecting devices that have a power connection. G 0.23 requires open communication interfaces like USB ports or SD card slots for example. In our framework, it has to be checked, if the IoT device have these components. If the device not have the hardware components, G 0.8 and G 0.23 not have to be considered. This process is illustrated by the following pseudocode.

```
for EACH IoT-Device x do
    SECURE G 0.1, G 0.2, G 0.3, G 0.4,
    G 0.12, G 0.13, G 0.21, G 0.24 ON x
    if x has power connection then
        SECURE G 0.8 ON x
    end if
    if x has open communication interface then
        SECURE G 0.23 ON x
    end if
end for
```

x is representing a certain IoT device which goes through the framework. SECURE indicates a function. If SECURE is ON, the hardware threat is affecting the IoT device and security practices has to be considered for a certain hardware threat like G 0.8 for example. Otherwise, the hardware threat is not affecting the device and no security practices has to be implemented for this threat.

V. DISCUSSION

The official security authorities consider different aspects of IoT security e.g., a secure planning, implementation and usage of IoT devices, data security, as well as software and hardware security. Our comprehensive review and comparison of three official IoT security standards, published by the BSI, NIST and ENISA has shown that the mentioned hardware threats are very similar within these standards. With our risk identification, we were also able to confirm that the mentioned hardware threats indeed affect a wide range of different application scenarios for IoT devices. Thus, it is meaningful to define a framework that includes these threats. However, suggesting appropriate security practices for these threats is not part of our framework, because they are already described in the BSI module SYS.4.4. It is also important to mention that further security measures are necessary. Our framework serves as a basic hardware protection. It includes IoT hardware threats that are affecting different IoT devices, regardless of their application scenarios or security requirements. Additional threats must be identified for each IoT device. In this way, our framework can be included into other security activities. For example, the BSI defines steps for a risk analysis in the BSI standard 200-3 [14] to identify additional threats and security practices according to specific application scenarios and security requirements. Our basic IoT hardware security framework could be implemented before the risk analysis. In this way it can be embedded into existing security concepts.

VI. CONCLUSION

This paper was motivated by the fact that official IoT security standards do not consider a uniform procedure for a basic hardware protection of IoT devices. The aim was to develop a basic IoT hardware security framework that can be implemented into existing security concepts. For this purpose, we analyzed three official IoT security standards, publishes by the BSI, NIST and ENISA. We compared which hardware threats are mentioned. These threats seem to be of great importance for IoT security in general. By performing a risk identification for four different IoT devices, we checked whether these threats really apply to different application scenarios. We were able to confirm the importance of these threats. In the next step, we used them to develop our basic IoT hardware security framework. This framework consists of a total of 10 hardware threats that are affecting different application scenarios for IoT devices. It can be used as a basic hardware protection for IoT devices, and it can be included into existing security concepts.

REFERENCES

[1] Business Wire, "Strategy analytics: Internet of things now numbers 22 billion devices but where is the revenue?" 2021.

[2] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[3] R. Gupta and R. Gupta, "ABC of Internet of Things: Advancements, benefits, challenges, enablers and facilities of IoT," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN).* IEEE, 2016, pp. 1–5.

[4] W. Zhao, S. Yang, and X. Luo, "On threat analysis of IoT-based systems: A survey," in *2020 IEEE International Conference on Smart Internet of Things (SmartIoT).* IEEE, 2020, pp. 205–212.

[5] V. Hassija *et al.*, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[6] K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A survey of distributed denial of service attack," in *2016 10th International Conference on Intelligent Systems and Control (ISCO).* IEEE, 2016, pp. 1–6.

[7] M. Hosseinzadeh, B. Sinopoli, and E. Garone, "Feasibility and detection of replay attack in networked constrained cyber-physical systems," in *2019 57th annual allerton conference on communication, control, and computing (Allerton).* IEEE, 2019, pp. 712–717.

[8] J. Kleinhans, "Internet of insecure things," https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf, Accessed March 2022, 2017.

[9] S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware Security in IoT Devices with Emphasis on Hardware Trojans," *Journal of Sensor and Actuator Networks*, vol. 8, no. 3, p. 42, 2019.

[10] J. Milosevic, N. Sklavos, and K. Koutsikou, "Malware in IoT software and hardware," *Conference: Workshop on Trustworthy Manufacturing and Utilization of Secure Devices*, 2016.

[11] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[12] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 32–37.

[13] L. I. P. Technik, "SONOFF S55 Wi-Fi Smart Waterproof Socket," 2020.

[14] Federal Office for Information Security BSI, "BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz," *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf, Accessed March 2022*, 2017.

[15] ——, "BSI IT Grundschutz Compendium Edition 2019," *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-it-gs-comp-2019.pdf, Accessed March 2022*, 2019.

[16] National Institute of Standards and Technology, "IoT Device Cybersecurity Guidance for the Federal Government," *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213-draft.pdf, Accessed March 2022*, 2020.

[17] ——, "IoT Device Cybersecurity Capability Core Baseline," *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf, Accessed March 2022*, 2020.

[18] ——, "IoT Non-Technical Supporting Capability Core Baseline," *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259B-draft.pdf, Accessed March 2022*, 2020.

[19] ——, "Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline," *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259C-draft.pdf, Accessed March 2022*, 2020.

[20] ——, "Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government," *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259D-draft.pdf, Accessed March 2022*, 2020.

[21] European Union Agency for Cybersecurity, "Baseline Security Recommendations for IoT," https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/, Accessed March 2022, 2017.

[22] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments ," *https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf, Accessed March 2022*, 2012.

[23] Reolink, "Most Popular 5MP PoE Security IP Camera," https://reolink.com/gb/product/rlc-410/ Accessed March 2022, 2021.

[24] X-Sense Innovations Co., Ltd., "X-Sense XS01-WT Wi-Fi Smoke Detector," https://www.x-sense.com/products/x-sense-xs01-wt-wi-fi-smoke-alarm Accessed March 2022, 2021.

[25] Sigfox Foundation, "Remote Signals Soil Temperature Monitor," https://partners.sigfox.com/products/remote-signals-soil-temperature-monitor Accessed March 2022, 2021.

[26] Allterco Robotics, "Make Your Home Smart," https://shelly.cloud/documents/catalogues/catalogue.pdf Accessed March 2022, 2021.