https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-276

New Methodology and Checklist of Wi-Fi Connected and App-Controlled IoT-Based Consumer Market Smart Home Devices

Franziska Schwarz, Klaus Schwarz, Reiner Creutzburg

Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany

Email: franziska.schwarz@th-brandenburg.de, klaus.schwarz@th-brandenburg.de, creutzburg@th-brandenburg.de

Abstract

Since its invention, the Internet has changed the world, but above all, it has connected people. With the advent of the Internet of Things, the Internet connects things today much more than people do. A large part of the Internet of Things consists of IoT controlled Smart Home devices. The Internet of Things and the Smart Home have become an increasingly important topic in recent years. The growing popularity of Smart Home devices such as Smart TVs, Smart Door Locks, Smart Light Bulbs, and others is causing a rapid increase in vulnerable areas. In the future, many IoT devices could be just as many targets. The many new and inexperienced manufacturers and the absence of established uniform standards also contribute to the precarious situation. Therefore, new methods are needed to sensitize and detect these threats.

In this paper, different existing approaches like those of the National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP) are combined with concepts of this work like the Smart Home Device Life Cycle. In the context of this paper, a universal 31-page question-based test procedure is developed that can be applied to any Smart Home device. Based on this new, innovative security checklist, the communication between device, app, and the manufacturer's servers, as well as the firmware of IoT devices, can be analyzed and documented in detail. In the course of this paper, also a hand-out in the abbreviated form will be created, which serves the same purpose.

Introduction

There are currently over 26 billion devices on the Internet of Things (Fig. 4). That is more than three devices per person on Earth. However, that is not all: this number is expected to triple in the next five to six years. A high fluctuation of manufacturers also accompanies this rapid growth. Also, microcontrollers for controlling state-of-the-art hardware are available to manufacturers for just a few cents per item. The entry into new technology has never been so affordable for consumers as today with smart light bulbs and sockets that are already available in the single-digit Euro range. However, these inexpensive, inconspicuous devices, in particular, have great potential not to be recognized as complex systems. Such a broad market inevitably encounters a diverse group of buyers, and so it is to be expected that many consumers will not regard the products of the IoT-Based Smart Home as complex computer systems with precisely these requirements and protection values. Fast, favorable developments from ever new manufacturers entering the market do the rest. The fast pace of the market hardly allows products to mature, and many inconsistent standards have an additional negative impact on security and privacy aspects. If all these conditions are taken together, an incredible amount of immature, insecure products from inexperienced manufacturers at low prices will meet inexperienced customers, who will be led into a feeling of functioning by apps and the cloud. So sockets and light bulbs with online connections are bought for little money and misjudged as conventional light bulbs and sockets. However, the life cycle of a smart light bulb differs significantly from that of a conventional one. IoT Devices based on Microcontrollers have memory functions and contain sensitive information. An inadvertently disposed of smart light bulb can open house and yard to attackers in conjunction with a smart door lock. With a conventional disposable lamp, of course, there is no need to think about such a thing. Based on these conclusions, we are developing an analysis methodology for the Security and Privacy of Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices. With this methodology, the current status of such Devices can be randomly checked on the one hand, and on the other hand, future users can be allowed to gain an impression of the hardware they are using themselves. To achieve this goal, we are combining two existing concepts into one and extending it with a holistic approach inspired by the life cycle of Smart Home devices.

Microcontroller

The most important component of the IoT devices considered in this paper is the microcontroller. It forms the core of all these devices. Furthermore, it controls the central functions of the individual devices as well as their entire communication with the network. A microcontroller generally consists of a microprocessor, memory, program memory, and other peripheral elements. Microcontrollers are designed to enable control or communication tasks with as few components as possible. All elements of a microcontroller are always tailored to its task [2]. Microcontrollers are embedded systems and, as such, often an invisible part of many devices and objects of daily life. For example, credit cards, washing machines, watches, and many other technical items such as the Internet of Things devices considered in this paper contain one or even several microcontrollers. Microcontrollers are interesting for the Internet-of-Things and especially for the Smart Home because they usually represent the smallest possible computer systems, which are cheap to produce on the

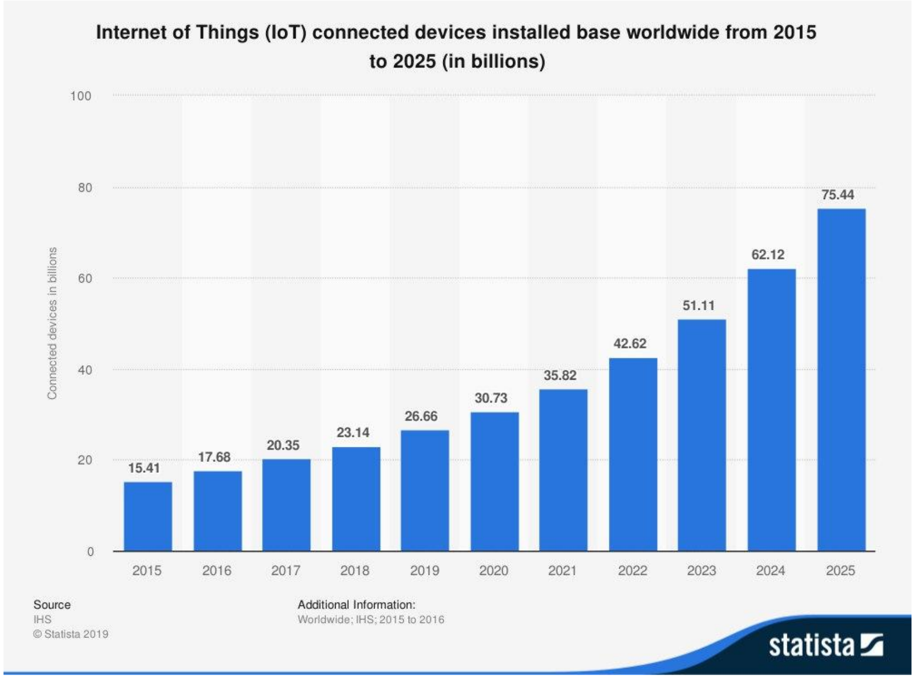


Figure 1. *IHS. "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions)". (2019): Statista. Web. Aug 20, 2019*

one hand and have enough power, on the other hand, to take over complex communication and control tasks. Microcontrollers usually do without an operating system and therefore have different requirements and needs for cybersecurity and privacy, especially in the context of the Internet of Things [3].

Architecture

Microcontrollers are usually single-chip computer systems that contain the core of a microprocessor and additional peripheral groups for measurement, control, and communication tasks. In most cases, the working and program memory is also located partially or completely on the same chip [3].

The microprocessor or core of a microcontroller contains an arithmetic unit, a control unit, a register set, and a bus interface and has registered with 4, 8, 16, or 32 bits. The processor clock of popular microprocessors, as they are currently found, is between 1 kHz and 200 MHz, which determines the processing speed.

Depending on the manufacturer and microcontroller family, the peripheral groups of a microcontroller consist of:

- different types of memory (ROM, RAM, Program Memory, Data Storage),
- different communication interfaces such as I^{2}C, I^{2}S, SPI, UART,
- ports for input and output (IO-Ports),
- counters and timer modules,
- an analog-to-digital converter,
- a digital-to-analog converter,
- integrated Wireless Local Area Network (WLAN).

Program Memory

The program memory of a microcontroller usually has its translated application program in non-volatile on-chip program memory. The size of the memory can range from a few bytes to several megabytes. In the following, the most common program memory types of microcontrollers are explained.

The Flash EEPROM is the most frequently occurring program memory type of microcontroller. The flash memory is either flashed in the development system (via USB JTAG) or via a serial connection through a bootloader. This is also possible if the microcontroller is installed in the system. The program can be easily changed at any time.

With the EPROM and EEPROM, it is possible to program the program at the customer. It remains changeable and is therefore suitable for the development and testing of programs.

With the OTP ROM, the microcontroller can be programmed once by the customer and is, therefore, more suitable for small series.

With the mask ROM, the program code is incorporated during the manufacture of the microcontroller (mask), and can then no longer be changed. This type of program memory is used in the production of large series.

Non-volatile RAM (NV RAM). The contents of the memory cells are transferred into EEPROM cells before being switched off. This type of program memory is rather rare.

Data Storage

The data memory of a microcontroller can contain the following elements:

- Register
  Consists of groups of flip-flops with common control within the CPU without bus transfer. The data transfer is high-speed, and the compiler tries to store the data at this location. The width of the registers can be 4,8,16 or 32 bits.
- General Data Area

This on-chip data memory is used for intermediate storage of program data (variables) that no longer fit into the register. This is usually SRAM since no refresh is required here.

- Stack
  The stack is part of the general data area and is used for short-term, intermediate storage of data. Access is via PUSH and POP.

Programming

Microcontrollers are usually programmed in the programming languages Assembler or C, which is the most commonly used high-level language for microcontrollers, as it allows programming very close to the hardware. Other possible programming languages are BASIC, Pascal, or C++ [3].

IoT Devices based on Microcontrollers

Many Smart Home devices have a certain resemblance to computers. The IP camera, which simultaneously runs a web server and allows hours of video to be stored on itself using a plug-in memory card. Other devices attract attention through the way they interact. There are smart loudspeakers that confront the consumer in the form of a "partner" through their special type of interaction. Smart vacuum cleaner robots also remain in the attention of the user in everyday life – at the latest when the dust container has to be emptied. Microcontroller-based devices are among the most inconspicuous devices in the Smart Home. Due to the nature of the microcontroller, the focus is on function, not interaction. Relays, sockets, and bulbs are generally there to be needed and to work, not to interact with. Thus, after a successful installation, these devices are usually forgotten until the moment they stop working. Besides, microcontroller-based Smart Home devices are often part of a more complex installation in which the focus is not on the individual relay but the entire heating control system, for example. An incandescent lamp with network functionality is often not seen as a computer controlling an array of LEDs but as a lamp. This lack of transparency can lead to fatal errors. This computer, which has access to the Internet and at the same time to the data traffic in the local network, also has a data memory containing sensitive information. Similar to a hidden microphone, the computer in the lamp hears the internal network traffic day after day and has advanced interception capabilities. This is a real catch for hackers and an even greater opportunity for cloud providers who collect data in a time where personal data is the currency of the Internet. The capabilities of microcontroller-based Smart Home devices can be classified as follows. Each microcontroller-based Smart Home device has:

- Transducer Capabilities,
  which make it possible to form an interface between the real and the digital world. Each Smart Home device offers at least one of the listed conversion capabilities.
  - Sensor Capabilities,
    which make it possible to perceive and digitize relevant data from the real world.
  - Actor Capabilities,
    that enable the digital world to execute commands in the real world.
- Interface Capabilities,
  which enable communication to and from the device. This includes communication from device to device as well as human interaction with the device.
  - Application Interfaces
    Enable an application to communicate with the device e.g., via a program interface. Communication via a human user interface, such as a physical switch or a status LED on the device, is also possible.
  - Network Interfaces
    Form the interface to the digital world. The connection to the cloud and thus to the Internet of Things. In this paper, this interface is based exclusively on a Wi-Fi connection.
- Assistance Skills
  These are dependable but mostly available capabilities that make it possible to extend or simplify the handling of the device.
  - Storage Capabilities
    Enable, for example, the storage of data such as access data or to bridge an offline phase.
  - Software-Based Extensibility
    Enables to extend the device with third-party software from an app store, for example.

Security

In general, security is freedom or resilience to potential damage and the absence of unacceptable risks. In the computer world, cybersecurity is divided into two related areas - the device and the data security [11].

Device Security

Device security is about protecting a device from being used for an unintended or harmful purpose. In the context of IoT-Based Smart Home Devices, the goal is both to prevent a device from tapping or compromising the internal network and to ensure that it is not taken over and misused from the Internet [12].

Data Security

Data security refers to the protection of the technical processing of information and is a characteristic of a functionally secure system. It is intended to prevent unauthorized data manipulation or the disclosure of information. [5].

Security Aspects

In addition to data and device security, several protection goals are required, which will be explained in detail below. In the context of electronic communication, the security aspects and protection goals mentioned in the following should always be considered in interaction. For example, it does not make sense to consider the integrity of the data and the authenticity of the data origin independently of each other. A message with changed content but known sender would be as useless as a message with unchanged content but faked sender.

Confidentiality

The aspect of confidentiality means that confidential information must be protected from unauthorized disclosure. [6].

Concerning IoT-based Smart Home devices, the confidential information is, for example, the data collected and shared with the vendor cloud. In particular, this includes data that enables access to the local network. In addition to this data and data on the user account, this can also include location data and user behavior, which could allow conclusions to be drawn about private life. An unencrypted transmission or the storage of user data in the firmware in plain text are possible weak points here.

Integrity

Data must not be changed unnoticed. All changes must be traceable [6].

Concerning IoT-based Smart Home devices, for example, the import of new firmware updates should be mentioned, which, among other things, can take place unnoticed in the background without the consumer noticing. Here it must be ensured that the modified firmware originates from the manufacturer and not from a potential attacker. However, it must also be ensured that data cannot be compromised during transmission from and to cloud servers. Systems should be so well secured that unauthorized access and modification of data is only possible and permitted from reliable sources.

Availability

Services, functions of an IT system, or information are available to the user at the required time [6].

Concerning an IoT-based device in the Smart Home area, it must provide its function without restriction. Many devices, such as smart light bulbs, lose their usefulness if they can no longer be switched or operated due to the unavailability of the service.

Authenticity

denotes the properties of authenticity, verifiability, and trustworthiness of an object [6].

For example, during the registration process, the identity of the logged-in person is checked and verified in the context of authenticity. In the case of an IoT-based device in the smart home sector, it must be ensured who is allowed to operate a device and who is not.

Non-Deniability

It requires that "no inadmissible denial of actions performed" is possible. It is important, among other things, for the electronic conclusion of contracts. It can be reached, for example, by electronic signatures [6].

Concerning this paper, the non-repudiation of communication can be seen in the protocols used by the individual Smart Home systems. Communication must be assignable to ensure that a device only receives commands that are intended.

Attributability

An action performed can be uniquely assigned to a communication partner [6].

About IoT-based Smart Home devices, the protection objective of accountability is somewhat contradictory. Concerning the collection of data that allows conclusions to be drawn about user behavior, it is essential that these cannot be unambiguously assigned and that the anonymity of the consumer is maintained.

Privacy

In addition to security, it is especially privacy that is threatened by the Smart Home in connection with the Internet of Things. Many smart devices deeply invade the privacy of the individual and collect vast amounts of personal data. Especially critical are the inconspicuous devices without complex user interfaces. While the smart loudspeaker, as well as the smart vacuum cleaner, attract attention through interactions, smart relays are embedded in the wall or hidden in the switch cabinet and still have full access to the local network and are capable of collecting personal data such as the user's movement data due to the type of use. The term privacy is, therefore, to be divided into two areas for this paper. On the one hand, the protection of privacy in the private sphere is of general interest; on the other hand, the processing of personal data is not to be neglected.

Privacy in Private Space

Privacy refers to the non-public area in which a person exercises his right to the free development of his personality without being bothered by external influences. The right to privacy is considered a human right (Article 12 "Universal Declaration of Human Rights") and is anchored in all modern democracies [1].

Processing of Personal Data

The protection of personal data is based on the principle of informational self-determination. This was laid down in the German Federal Constitutional Court ruling on the census. Privacy must be protected, i.e., personal data and anonymity must be preserved. The protection of natural persons in the processing of personal data is a fundamental right. Under Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), every person has the right to the protection of personal data concerning him or her. The principles and rules on the protection of personal data must be ensured. This includes fundamental rights and freedoms and, in particular, the right to the protection of personal data regardless of nationality or place of residence. In addition to these rights to privacy and the processing of personal data, the General Data Protection Regulation (GDPR) continues to regulate the processing of personal data. Its purpose is, on the one hand, to ensure the protection of personal data within the European Union and, on the other hand, to ensure the free movement of data within the European internal market. In addition to the many regulations that the European laws and with them the General Data Protection Regulation (GDPR) entail, the following are of particular relevance for this paper.

Marketplace Principle

The market place principle means that European Data Protection Law also applies to Non-European companies if they offer their products within the European Union [14].

Right to be Forgotten

The right to be forgotten gives individuals the right to request the deletion of all personal data concerning them at any time if the reasons for the data retention cease to exist. It also obliges companies that process personal data to delete this data if there is no longer a reason for storing it [14].

Privacy by Design, Privacy by Default

With the General Data Protection Regulation, European data protection law also brings with it the principles of data protection through technology design (Privacy by Design) and data protection-friendly basic settings (Privacy by Default). On the one hand, companies that process personal data must ensure that data economy is ensured during the development of software and, on the other hand, data-saving settings must ensure that a consumer does not have first to try the settings of an application to prevent the collection of personal data [14].

Principle of Transparency

Another principle that goes hand in hand with the basic data protection regulation is the principle of transparency. These are actions called for in several articles of the Regulation. So has:

- in accordance with Art. 15, every person has the right to access all data concerning him.
- According to Art. 12, the information must be provided in a “precise, transparent, comprehensible and easily accessible form in clear and simple language”.
- According to Art. 13 and 14, each data subject must be provided with comprehensive information in a data protection declaration when collecting data, including the purpose, recipient, and person responsible for data processing, duration of data storage, rights to correct, block and delete data, and use of the data for profiling purposes. If the purpose changes, the person concerned must be actively informed.
- According to Art. 16, the data subject has a right to rectification of false data and according to Art. 18 a right to limitation (“blocking”) of data processing if the accuracy or basis of the data processing is disputed.

It should be noted; however, that data subjects themselves are obliged to take active care of who and how their data are processed and to claim their rights.

Right to Data Transferability

The right to data portability confers on individuals the right to obtain at any time data relating to them, which they have transmitted in a structured, standard, and machine-readable format [14].

OWASP Internet of Things Top 10

The Open Web Application Security Project (OWASP) is a non-profit organization dedicated to making the Internet more secure. “OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted” [7]. For this purpose, the project regularly publishes information and tools that enable interested parties to define security risks in software. The OWASP Internet of Things (IoT) Project was created for this purpose. “The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies” [8]. In this context, the OWASP regularly publishes the “Internet of Things (IoT) Top 10”, the second edition of which appeared in 2018 [9]. Since this paper has a specific definition for IoT-based Smart Home devices, it works with the old version of the “Internet of Things (IoT) Top 10 2014” because of the much higher compatibility [9]. The older version was created at the time of release with the background of addressing developers, manufacturers, businesses, and consumers alike. In the new version, the focus has shifted away from consumers and more towards helping to improve the development process. The decision was made to use the older version in order to meet not only the requirements on the special design of the hardware but also the reusability of this paper.

The “Internet of Things (IoT) Top 10 2014” [9] specifies the following points to observe and avoid when handling IoT devices:

- Insecure Web Interface,
- Insufficient Authentication/Authorization,
- Insecure Network Services,
- Lack of Transport Encryption,
- Privacy Concerns,
- Insecure Cloud Interface,
- Insecure Mobile Interface,
- Insufficient Security Configurability,
- Insecure Software/Firmware,
- Poor Physical Security.

NIST Considerations

The National Institute of Standards and Technology is a federal agency of the United States of America. The Institute is part of the Department of Commerce’s technological administration and is responsible for standardization processes. To this purpose, the agency regularly issues publications on a wide range of topics. Of particular importance for this paper is the publication “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks”. [10] hereinafter referred to as “NISTIR 8228”. The purpose of NISTIR 8228 is to assist organizations in managing risks associated with the use of IoT equipment. The focus is clearly on instructions for companies. However, since the interpretation of “NISTIR 8228” is not limited to the definition of IoT devices and thus also focuses on consumer and Smart Home devices, the decision was made to include NISTIR 8228 in this paper. The “NISTIR 8228” also provides the division of security into device and data security, which also forms the basis of this paper in a modified form. It was also the basis for setting up the capabilities of microcontroller-based Smart Home devices.

The following “NISTIR 8228” notes are incorporated into this paper as a means of identifying and addressing security and privacy issues:

- Understand the IoT device risk,
- Adjust organizational policies and processes,
- Implement updated mitigation practices.

Smart Home Device Life Cycle

The life cycle of a Smart Home device after the definition of this paper is complex. For example, in the research for this work, it turned out that not a single manufacturer of the investigated products examined disposal instructions that indicate - due to the nature of those devices - that these products may contain private data and how to delete it. When the editors of the British daily newspaper The Guardian were ordered by the British government in 2013 to destroy a notebook with the aim of absolute

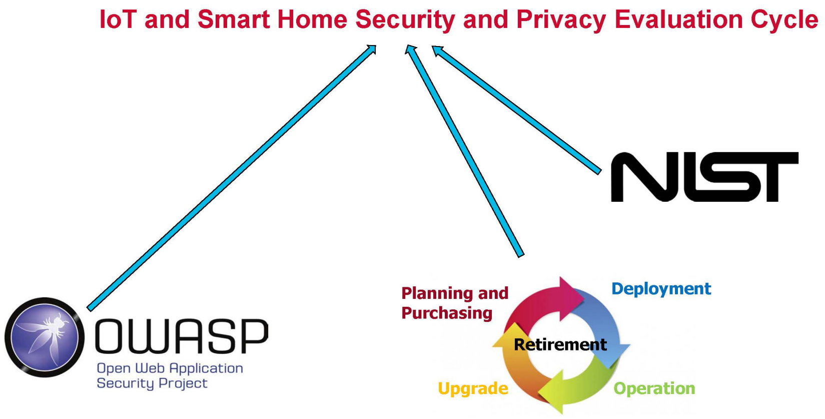


Figure 2. IoT and Smart Home Security and Privacy Evaluation Cycle

data erasure, not only was the hard disk erased, but microchips were also deliberately destroyed in a wide variety of places. Tools such as drills and angle grinders were used to purposefully destroy parts such as the power and keyboard controllers to ensure that all data was erased. "In fact, the Federal Office for Information Security specifies entire catalogs for the selection of suitable methods for safe deletion depending on the protection requirements" [13]. Without appropriate information, consumers cannot see how devices can be disposed of in a manner that protects the private sphere. Based on this assumption, this paper establishes a paradigm that Smart Home products have a complex life cycle that contains complex requirements at every stage. This life cycle is defined below.

The Smart Home Device Life Cycle consists of the following components:

- Planning and Purchasing,
- Deployment,
- Operation,
- Upgrade,
- Retirement.

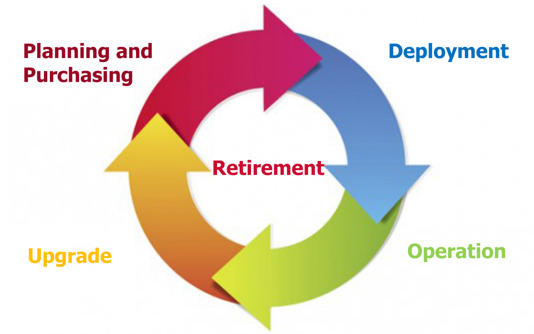


Figure 3. Smart Home Device Life Cycle

Smart Home Security and Privacy Evaluation Cycle

Not only in the Smart Home is the complex Internet of Things confronted with a complex mixture of consumers. The Smart Home devices, according to the definition of this paper, belong to the smallest, cheapest, and most unshakably consumer market devices and therefore, also have the greatest potential to overtax consumers with their requirements regarding security and privacy. The Smart Home Security and Privacy Evaluation Cycle are made up of the three building blocks mentioned above to have the broadest possible coverage and, at the same time, provide consumers with easily comprehensible means. These have to be repeated in each life cycle section. First, however, there is a general pre-consideration that must be made. The capabilities of the device have to be considered. Data exchanging devices after the definition of this paper does not necessarily always have the same protection value. So a simple temperature sensor has used to measure the outside temperature apart from the data to local Wi-Fi, hardly any data worth protecting. A temperature sensor in the house, on the other hand, has information worth protecting. Thus it could be read from the temperature when someone is at home and when not, as well as sleeping and waking times and personal habits. For this purpose, the need must be planned first exactly. The rules for this planning are as follows:

- **Consider the Device Capabilities**
  - **Transducer Capabilities**
    These abilities make it possible to form an interface between the real and the digital world. Here it has to be considered whether only sensor or actor capabilities are needed or whether the device has to have a mixed form of capabilities. The more of these capabilities are available, the higher the protection requirement of a device increases. As already described in the example, sensor capabilities, for example, have a different protection value depending on the location. If a switch is added to the outdoor temperature sensor, protection against unauthorized switching operations must also be considered here.
  - **Interface Capabilities**
    These capabilities enable communication with the device from person to person as well as communication from device to device. It is necessary to consider which application interfaces are required. If the device must have a display, the protection value is higher than without display. Furthermore, it must be consid-

ered how the device is to be integrated into the network. Is it mandatory to have the device in the home network, or is it possible to operate it in the guest network. Regardless of the Smart-Home device's network, it must also be checked in which network and on which device the Smart-Home device's app must be operated. By connecting to the Internet of Things, both ends, i.e., both the Smart Home device and the app, communicate with the cloud. If one of the two ends is operated in the home network and the other in a guest network, the cloud provider theoretically has information about two networks.
  - **Assistance Skills**
    These capabilities are often found as a small added value in many devices. For example, a Smart Home device can usually be extended with software features in a kind of App Store. Mostly these extensions are done by third-party providers similar to Amazon's smart loudspeaker Alexa. Developers from all over the world make so-called skills available there, which ensure that the data runs via the developer's server in addition to the manufacturer's cloud.

Once these preliminary considerations have been made, the life cycle must be processed. Each stage of the cycle is worked out in such a way that consumers can also understand the necessary considerations and test steps. For this purpose, the building block from the "NISTIR 8228" was preceded by the OWASP "Internet of Things (IoT) Top 10" in each stage and extended by the item "Update Policy". It should be noted that each step in the life cycle should only be processed immediately during entry. Possible pre- and post considerations can lead to wrong results. So it is quite possible to think about the deployment of a smart device before buying it. However, the physical security of a device may be different after purchase, during setup, for example. By working through the checklist step-by-step and on time, unpleasant compromises can be avoided as far as possible.

Planning and Purchasing

This step must be carried out directly before and during the purchase. It is possible that certain questions from this step cannot be answered during the purchase. The questions in this step are only considerations. First of all, it is necessary to determine which partner will be chosen. Unlike the world of non-smart products, where there are few points of intersection with a manufacturer after the purchase, the partnership with a manufacturer in the world of smart products through cloud connectivity and after-sales services is just beginning.

- **Considerations in this Step:**
  - **Update Policy** For this step, it is necessary to find out what the update-policy of the manufacturer is like. This is mainly research work. Does the manufacturer indicate a support plan? How was the update-policy for other products of the manufacturer? If the manufacturer only releases updates for a short time or no updates at all for the product, known security gaps cannot be closed sooner or later. At this point, it is advisable to either modify the product by the consumer himself or to dispose of the product if this cannot be guaranteed.
  - **Privacy Concerns** Also, this step is at this time in the life cycle rather than consideration and needs research. In order to choose the right manufacturer as a partner, it is important to build trust. It should be researched whether the manufacturer has attracted attention in the past through privacy and security incidents and how he has responded to them. It is better to choose a manufacturer who has attracted attention due to an incident, but who has improved, than a completely unknown manufacturer, who may even be lost soon in the high fluctuation of manufacturers. It is also important to consider what kind of business the manufacturer is doing. Google, for example, is not a smartphone manufacturer but earns its money with data.
  - **Insecure Cloud Interface** In this step, one has to find out everything about the cloud used or operated by the manufacturer. There are three scenarios. In the first scenario, the manufacturer is also the cloud operator. This is the most data-efficient constellation. However, a manufacturer with a focus on hardware is not necessarily a good, reliable, and above all experienced cloud operator in every case. In the second scenario, the hardware manufacturer has found a specialized cloud provider. This scenario is probably the most common in practice. Here it is particularly likely that both the manufacturer and the cloud operator will have access to the device's data in the cloud. In the third scenario, the cloud manufacturer has a hardware manufacturer for production. This constellation has the advantages of the first scenario without its disadvantages.
  - **Insecure Mobile Interface** In this step, one has to find out everything about the app of the manufacturer or the product. It is a good idea to check out the App or Play Store in advance to check other users' ratings. What impression does the App? How is it translated? If the reviews are consistently positive, but there are no text reviews, they are often fake reviews. What have other users experienced? At this point, one can also use the update history in the shop to see what the update-policy of the manufacturer is like. Here one can also see how the manufacturer has reacted to possible critics in reviews.
  - **Insecure Software/Firmware** In this step, one has to find out everything about the firmware and any other software for the device one wants to buy. For example, some projects have already dealt with the product. Has a community been found that offers an alternative firmware that can be used in case of missing updates or generally as an alternative to the original firmware? It is generally better to prefer products that have an active community.

- **Understand the IoT device risk** After extensive research in the first step of the life cycle, it is important to have a comprehensive impression. A general impression of the risk allows a better adaptation in the next step.

- **Adjust policies and processes** At this point, it is important to understand that never everything is exactly right and safe. It is important to know the risks and adapt to the user's actions accordingly. If, for example, a device has an active community with a first-class alternative firmware, but the original firmware is unreasonable, it is still possible to make a positive purchase decision if the user has the appropriate skills.
- **Implement updated mitigation practices** In conclusion, it is important not only to do good research and consider the issues but also to adapt the active approach accordingly. Only when everything has been done so far, the next step of the life cycle can be taken.

Deployment

This step must be performed during setup. Many points and questions are simply difficult to answer in advance. After all the basic considerations have been made in the first step of the life cycle based on research, many points in this step must be checked. It is also necessary to consider whether the right partner has been chosen with the chosen manufacturer, or whether the right of return may even have to be exercised because fundamental considerations cannot be met or irreconcilable compromises arise.

- **Considerations in this Step:**
  - **Update Policy** The update-policy of the manufacturer is of enormous importance and, therefore, to be considered in most sections of the life cycle. At this point, it should be checked if there is an update to install. Usually, the manufacturer produces specific hardware in a certain revision. The date of this revision is then also the release date of the firmware on the device. If the manufacturer has, in the meantime, found errors and repaired or closed security gaps, this is to be regarded as particularly positive.
  - **Insecure Web Interface** In this step, there is the first time actual contact with the software and the interfaces of the manufacturer. At this point, it is important to check who has access to a possible web interface and how it is secured. If the IoT device has a website in the local network, the demand for the protection of this interface is not as high as in the case of a web interface for remote access. However, it is always important to consider whether the default password and username can be changed. Are special characters allowed? How long can credentials be? Is there a recovery mechanism, and if so, how is it implemented? If, for example, one has to press a hardware button to reset the data, this is better than if one only needs an e-mail address. However, the e-mail address is preferable if the device is otherwise publicly accessible, for example, because it was set up outdoors.
  - **Insufficient Security Configurability** In this step, it is important to consider who has access to the IoT device and how access can be shared. Most devices offer to allow multiple users with different accounts to access the device. This feature is convenient so that it is not always necessary to find exactly the smartphone on which access to the specific device is set up. However, it may also allow unauthorized third parties to access the device. The release of access to a device must, therefore, be carefully checked. If, for example, there is a notification for new access logins, this can be regarded as positive. If a device can be easily registered as an additional administrator, the right of return should be considered.
  - **Poor Physical Security** This step is not intuitive at first glance. Since all smart devices with access to a Wi-Fi network keep the credentials of the Wi-Fi network in memory and it is not easy to see whether it is encrypted, it is important to check carefully whether it is possible to compromise the device without this being apparent afterward. If housing is completely glued or there are security stickers, this is to be regarded as rather positive. Also, other anti-tamper facilities are positive. In the absence of protective measures, the location of the device should be carefully considered.
  - **Insufficient Authentication /Authorization** Here it has to be checked how the authentication and authorization, in general, are doing. What possibilities of access are there on the web, via the device, in the cloud, and the app? What about the authorization of co-users? What are the rules for credentials? Can a third factor be set up? If the setting options here do not fit the user's complete satisfaction, it is advisable to return the device.
  - **Insecure Cloud Interface** In this step, it has to be checked whether there is direct cloud access or not. If so, the possibilities of authentication have to be checked. Cloud access can be used for remote maintenance even without the app. But if only weak or even default user data is possible, the gate is open for anyone who can use a search engine, and it is advisable to return the device
  - **Insecure Software /Firmware** In contrast to the previous steps, this step should not be considered trivial. Nevertheless, it is important to make a decision. First, check whether it is possible to update the device at all. Are there specific entries to check for updates in the app? If possible, check how an update is transferred. If it is transferred via HTTP and is also unsigned, it can theoretically be compromised by any participant on the Internet. For this, it is a good idea to consult the work of the community on the device. Information can often be found on project pages about the device. However, it is also advisable and is expressly recommended to monitor the data traffic of the IoT devices permanently. This way, the endpoints of the device can be easily checked and monitored.
  - **Privacy Concerns** In this step, the general feeling of safety in connection with the device is to be checked once again. Are there any compromises in connection with safety, and is it perhaps worthwhile to use a different device? Since these devices are permanently on the Internet and often move into the background during normal use with normal functionality, it is important to consider carefully.

- **Insecure Mobile Interface** At this point, it is important to take a close look at the security settings of the app. How to set and improve credentials in the app. What permissions does the app ask for? Does the app ask for location data immediately and cannot even be opened without it? Is every single element of the app downloaded from the Internet, or does the app also work offline or only in the local network? This consideration seems trivial, but images and style sheets, even within an app, are often loaded without encryption and allow manipulation on the one hand and tracking of user behavior on the other. Is it possible to set up the device in the app without using the cloud or only over the local network?
- **Insecure Network Services** The considerations of this step are not necessarily trivial either. It is important to find out how the device communicates, whether this is encrypted, and, if so, how strong the encryption is. On the one hand, this can be found out through the community of the device. Products with an active community have often developed their interfaces so that these questions can be found in the corresponding documentation of the communities. However, it is also possible to clarify these questions via a port scan of one' s own. Long-term monitoring of the traffics of the particular device is also advisable and explicitly recommended. This way, it can be guaranteed that traffic always behaves the same in the long run and that possible changes are dealt with.

- **Understand the IoT device risk** After setup, it is particularly important that the risk taken is considered, and the system is prepared for long-term use. At this point, it is advisable to consider carefully whether the unit should be kept or whether any compromise is too great.
- **Adjust policies and processes** At this point, it is to be understood again like the first time that never everything is exactly right and safe. It is important to know the risks and adapt to the user's actions accordingly. If a device is not physically safe, it can still be operated in a suitable cabinet.
- **Implement updated mitigation practices** In conclusion, it is important not only to do good research and consider the issues but also to adapt the active approach accordingly. Only when everything has been done in advance, the next step of the life cycle can be taken.

Operation

This step must be performed after setup during normal operation. Since these devices run for a long time, it is important to understand that this step in the life cycle must be performed permanently and above all regularly. After a device has been taken over by a vulnerability, for example, the traffic changes significantly. This can be determined quickly by continuous observation. If a device is simply operated without appropriate monitoring, it must inevitably be possible to rely on updates from the manufacturer and the security of the entire system.

- **Considerations in this Step:**
  - **Update Policy** In this step, one has to check permanently if the manufacturer continues to make updates available for the device. If the support for the device has expired, the device should either go to the last step of the life cycle or at least be monitored closely by permanent monitoring.
  - **Insecure Web Interface** If it was determined during setup that there is a web interface, check whether the passwords are still secure. Multiple used passwords appear sooner or later in databases and are automatically used by hackers as a gateway in brute force attacks, in which millions of user data are tried through. If an existing web interface is no longer used, it is advisable to check whether it can be switched off.
  - **Lack of Transport Encryption** As already recommended before, it is a good idea to monitor Smart Home devices permanently. Just like a virus scanner runs on most home computers. Although the device's traffic may be encrypted, it can change over time if the cloud operator changes its nodes.
  - **Insufficient Security Configurability** In this step, one has to check the balance of the previous life cycle step again. If the security during the setup was sufficient, it is to check whether it still is at present. For example, encryption standards often prove to be no longer secure. If a compromise was made here in the previous step, it is necessary to check here whether this is still acceptable.
  - **Poor Physical Security** At this point, check how the physical stability of the device has changed. A device that is permanently exposed to changing or extreme environmental conditions, for example, may deteriorate over time. It is also important to check whether there are any indications that the device may be compromised.
  - **Insufficient Authentication /Authorization** The consideration of the previous step must also be checked here. Are the requirements for authentication and authorization still sufficient, or have standards changed significantly? If a compromise has been reached, it has to be rechecked, whether it is still acceptable.
  - **Insecure Cloud Interface** Once again, the consideration of the previous step must be examined here. If the possibilities of authentication and authorization are still sufficient, has the cloud access changed? If a compromise was made in the previous life cycle step, check again whether it is still acceptable.
  - **Insecure Software /Firmware** The considerations of the previous life cycle step must also be checked here. Are there any publications on security vulnerabilities of the respective manufacturer or even of the specific device? Is there a community around the device, and is it still active? Can the firmware be updated or replaced by a community development? If a compromise was made in the previous life cycle step, check again if it is still acceptable.
  - **Privacy Concerns** What about the general feeling of security? Are there regular updates? Does the device still feel safe? Have credentials been used several times, and are there accesses for third parties that are

no longer needed? Should there be any concerns here, the device must be transferred immediately to the last step of its life cycle. If a compromise was made in the previous life cycle step, check again whether it is still acceptable.
    - **Insecure Mobile Interface** At this point, one should check how the app has changed over time. Have there been, and are there updates for the app? What is the rating of other users for the app? What about the permissions the app requests? Is it now possible to operate the device exclusively in the local network? What about loading images and style sheets? Does the app work offline? If a compromise was made in the previous life cycle step, one has to check again whether it is still acceptable.
    - **Insecure Network Services** In this step, check the communication status of the device. Has monitoring been set up? Has the traffic changed? Is encryption now or still available? If a compromise was made in the previous life cycle step, check again whether it is still acceptable.
- **Understand the IoT device risk** In long-term operation, it is now of particular importance that the risks taken are constantly considered and that the device is kept in view for the long term. At this point, it is once again advisable to consider carefully whether the device should be kept or whether a possible compromise is too big, and the device should be transferred to the last life cycle step.
- **Adjust policies and processes** At this point, it is to be understood again, as already with the previous times, that everything is never exactly correct and safe. It is important to know the risks and adapt to the user's actions accordingly. With excellent monitoring, many devices can still be operated for a while until the compromises finally become too big.
- **Implement updated mitigation practices** In conclusion, it is important not only to do good research and consider the issues but also to adapt the active approach accordingly. Only when everything has been done so far, the next step of the life cycle can be taken.

Upgrade

This step must be performed if the device is to be upgraded in any way during normal operation. This is usually done through software from a manufacturer's store where third-party vendors provide the software. At this stage of the life cycle, it is important to understand that if the upgrade is third party software or software from the vendor that uses third-party services, all relevant data will automatically be shared with a third party. This means that any considerations of trust, security, and risk must also be made concerning the third party.

- **Considerations in this Step:**
    - **Update Policy** The update-policy of the third-party vendor is of enormous importance and therefore has to be checked in this life cycle section. At this point, it should be checked if there is an update available when setting up the upgrade. How active is the developer of the upgrade, and where is he based? Can the provisions of the European Data Protection Act be fulfilled?
    - **Insecure Web Interface** Does the upgrade give access to a web interface? At this point, it is important to check who has access to a possible web interface and how it is secured. If the IoT device, e.g., receives a website in the local network as a result of the upgrade, the requirement for the protection of this interface is not as high as in the case of a new third-party web interface for remote access. What about the credentials? Check whether the default password and username can be changed. Are special characters allowed? How long can credentials be? Is there a recovery mechanism, and if so, how is it implemented?
    - **Lack of Transport Encryption** As already recommended before, it is a good idea to monitor Smart Home devices permanently. Just like a virus scanner runs on most home computers. Although the device's traffic may be encrypted, it can change over time if the cloud operator changes its nodes. This step is even more recommended when upgrading with third-party software or services.
    - **Insufficient Security Configurability** In this step, it is important to consider who now has access to the IoT device and how access can be shared. Most devices offer to allow multiple users with different accounts to access the IoT device. Does the upgrade allow a new type of access for third parties? How do I configure it? What are the security settings of the upgrade in general? For example, is there a notification for new access logins? Are there any security settings at all? Are security settings required?
    - **Insufficient Authentication /Authorization** Here it is necessary to check the general status of the authentication and authorization of the upgrade. What are the possibilities of access through the upgrade on the web, via the device, in the cloud, and the app? What about the authorization of co-users, were they added by the upgrade? What are the rules for credentials, were they changed by the upgrade? Can a third factor be set up for or by upgrade features? If the settings here are not to one' s complete satisfaction, it is advisable not to upgrade or to uninstall it.
    - **Insecure Cloud Interface** Does the third-party provider use or offer cloud services? In this case, find out everything about the cloud used or operated by the third party. Can the provisions of the European Data Protection Act be complied with? In which countries do the cloud endpoints lie? Which and, above all, how much data is stored? Is the data passed on to third parties? Is there a policy to which the third party provider is committed?
    - **Insecure Software /Firmware** How does the app's software change? Will a new app be added? What about the update-policy of the third party? How does the firmware of the device change? Will there still be updates for the device? Who will provide updates for the device in the future? Will there be updates from third parties in the future?

  - **Privacy Concerns** Again, it is important to understand that choosing a third party is choosing another partner. It is important to build trust to choose the right third-party partner. It should be researched whether the third-party provider has attracted attention due to incidents related to privacy and security, and if so, how he reacted. It is better to choose a third-party provider who has previously attracted attention through an incident, but has improved, than a completely unknown one, who may even be subject to high fluctuation soon. It is also important to consider what kind of business the third party is doing. For example Facebook is a social network, but earns its money with targeted advertising and the data of its participants.
  - **Insecure Mobile Interface** In this step, it is important to find out everything about the third-party app or product if it exists. It's a good idea to check the App Store or Play Store in advance to check other users' ratings. What impression does the App make? How is the app translated? If the reviews are consistently positive, but there are no text reviews, they are often fake reviews. What experiences have other users had? At this point, the update history in the store can also be used to see what the update-policy of the third-party provider looks like. One can also see whether the third-party provider reacted to any criticism in ratings.
  - **Insecure Network Services** In this step, check how the communication of the device changes. Has monitoring been set up? Has the traffic changed? Is third-party encryption available? If a compromise has to be made here, it is worth, not upgrading.

- **Understand the IoT device risk** Especially after an upgrade has been installed, it is particularly important that the risks taken are constantly evaluated and that the device remains monitored over the long term. At this point, it is advisable to consider carefully whether the upgrade should be kept or whether a possible compromise is too big, and the upgrade is easier to uninstall.
- **Adjust policies and processes** At this point, it is to be understood again, as already with the previous times, that everything is never exactly correct and safe. It is important to know the risks and to adapt one' s actions accordingly. With excellent monitoring, many devices can still be operated for a while until the compromises finally become too big.
- **Implement updated mitigation practices** In conclusion, it is important not only to do good research and consider the issues but also to adapt the active approach accordingly. Only when everything has been done so far, the next step of the life cycle can be taken.

Retirement

This step must be performed when the device has reached the end of its life cycle. It is especially important and quickly neglected because it is not easy to identify that Smart Home devices contain personal and sensitive information. Also, most deletion methods are not trivial. In the example of the notebook of the British Guardian and the British domestic intelligence service, which was about to erase the device, the microchips had to be shredded into pieces no larger than three millimeters after forcible removal by drills and angle grinders. This procedure is not advisable for a consumer. However, it is advisable to reset the device several times before disposal or to set it up with incorrect information.

Keine Leuchtstoffröhren einlegen
Sparlampen bitte unverpackt einlegen.
lightcycle.de

Figure 4. Free bulb recycle box

- **Considerations in this Step:**
  - **Poor Physical Security** What about the physical security of the device now? Can data in the device simply be accessed, or is the device so glued that it is destroyed when opened? Is it certain that the destruction caused by violent opening is sufficient? Can violent opening itself be used as a method to delete the device safely?
  - **Insufficient Authentication /Authorization** In this step, it is about the consideration of further use by an unauthorized third party. How secure were passwords for accounts and shares? Can accounts simply be transferred after use? Could the account be deleted? What about data and accounts with third-party providers?
  - **Insecure Software /Firmware** What about the firmware on the device? Was the device encrypted? Is it safe that all memory and any data partitions were encrypted? What about the app's data?
  - **Privacy Concerns** At this point, it is once again a question of weighing up whether the manufacturer was the right partner? How does the manufacturer deal with the remaining data after separation from the device? How much data does the manufacturer hold, and how long is it stored? Is it possible to have personal data sent in? Can one rely on the deletion of personal data? What about data from third parties? Is my data being, or has it been sold to third parties?

- **Understand the IoT device risk** Arrived at the end of the life cycle of a Smart Home device, it is mainly about privacy concerns and how the selected partners in the form of manufacturers and third parties behave towards the consumer's data. How much data was stored when, how long is it held, and how can it be deleted? These are central questions in this step of the life cycle. In addition to the data in the cloud/clouds, the remaining data on the device is also important. In addition to multiple resetting and setting up with incorrect data, the consumer has only a rough tool at the moment to make sure that all data is deleted locally. During the research for this paper, no manufacturer-supplied proper disposal instruction.
- **Adjust policies and processes** At this point, it is to be understood again, as already with the previous times, that everything is never exactly correct and safe. It is important to know the risks and to adapt one' s actions accordingly. With excellent monitoring, many devices can still be operated for a while until the compromises finally become too big.
- **Implement updated mitigation practices** In conclusion, it is important not only to do good research and consider the issues but also to adapt the active approach accordingly. Only when everything has been done so far, the next step of the life cycle can be taken.

Summary and Outlook

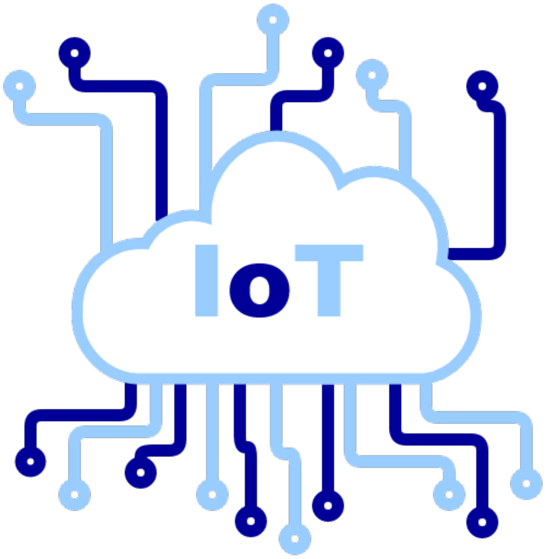
Since the invention of the internet it has changed the world, but most of all it has connected people. With the advent of the Internet of Things, the Internet now connects many more things than people. This is what can be said when it comes to describing what the Internet of Things is. The Internet of Things also includes smart home devices. To investigate such devices in terms of privacy and security, various existing approaches such as those of the National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP) have been combined with concepts from this work such as the Smart Home Device Life Cycle. In this way, the "Smart Home Security and Privacy Evaluation Cycle" was created, which can serve as a basis for further investigations. With a few prerequisites, a thing can become part of the Internet. One of the results of this work is that risks and side effects in terms of security and privacy for the consumer cannot simply be determined intuitively. It can be considered unlikely that consumers will ask themselves almost 170 questions before using a light bulb. However, this work shows that this is necessary. Only those who ask themselves at each stage of the life cycle of a smart home device how its features and capabilities correlate with the security of the data, the device and the privacy in the personal space can respond appropriately.

Sustainable standards and appropriate regulation leading to security, technical interoperability, data portability, and the necessary level of privacy are essential first steps to enable trusted systems. The market for IoT devices is growing fast and remains great hope for the future. If these standards can be successfully established and the devices regulated, the Smart Home can become an exciting next step in the history of the Internet. If this is not achieved as before, 75 billion devices in the next five to six years will be the same number of potential targets for attacks of all kinds, making the Internet a worse place. Today's consumers, with a strong desire for security and privacy, can make a direct contribution to preventing this from happening.

Appendix

The Appendix includes the Security and Privacy Checklist flyer for information about the investigation of Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices.

Security and Privacy Investigation of Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices



To investigate security and privacy aspects of Wi-Fi Connected and App-Controlled IoT-based Smart Home Devices, various existing approaches such as those of the National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP) were combined with concepts such as the Smart Home Device Life Cycle. For a representative result, a universal test procedure is developed that can be applied to any Smart Home Device. This Security checklist provides an overview of the considerations that should be made during the various stages of a Smart Home Device's Life Cycle to mitigate privacy and security concerns.

Smart Home Security and Privacy Evaluation Cycle

Consider the Device Capabilities

- Transducer Capabilities
  - Sensor Capabilities
  - Actor Capabilities
- Interface Capabilities
  - Application Interfaces
  - Network Interfaces
- Assistance Skills
  - Storage capabilities
  - Software-based Extensibility

Checklist

Planing and Purchasing

- Considerations in this Step
  - Update Policy
  - Privacy Concerns
  - Insecure Cloud Interface
  - Insecure Mobile Interface
  - Insecure Software/Firmware
- Understand the IoT device risk
- Adjust policies and processes
- Implement updated mitigation practices

Deployment

- Considerations in this Step
  - Update Policy
  - Insecure Web Interface
  - Insufficient Security Configurability
  - Poor Physical Security
  - Insufficient Authentication /Authorization
  - Insecure Cloud Interface
  - Insecure Software/Firmware
  - Privacy Concerns
  - Insecure Mobile Interface
  - Insecure Network Services
- Understand the IoT device risk
- Adjust policies and processes
- Implement updated mitigation practices

Operation

- Considerations in this Step
  - Update Policy
  - Insecure Web Interface
  - Lack of Transport Encryption
  - Insufficient Security Configurability
  - Poor Physical Security
  - Insufficient Authentication /Authorization
  - Insecure Cloud Interface
  - Insecure Software/Firmware
  - Privacy Concerns
  - Insecure Mobile Interface
  - Insecure Network Services
- Understand the IoT device risk
- Adjust policies and processes
- Implement updated mitigation practices

Upgrade

- Considerations in this Step
  - Update Policy
  - Insecure Web Interface
  - Lack of Transport Encryption
  - Insufficient Security Configurability
  - Insufficient Authentication /Authorization
  - Insecure Cloud Interface
  - Insecure Software/Firmware
  - Privacy Concerns
  - Insecure Mobile Interface
  - Insecure Network Services
- Understand the IoT device risk
- Adjust policies and processes
- Implement updated mitigation practices

Retirement

- Considerations in this Step
  - Poor Physical Security
  - Insufficient Authentication /Authorization
  - Insecure Software/Firmware
  - Privacy Concerns
- Understand the IoT device risk
- Adjust policies and processes
- Implement updated mitigation practices

References

[1] Saleh, I., Ammi, M., Szoniecky, S.: *Challenges of the Internet of Things.*, Wiley 2018.

[2] Kaler, R. S.: *Mikroprocessors and Microcontrollers.* IK Internat. Publishers 2014.

[3] Kant, K.: *Mikroprocessors and Microcontrollers.* PHI Learning Private Ltd., Delhi 2012

[4] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Catalogues 15 Version 2015.* (2015): `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf` (last access: August 27, 2019).

[5] Schmeh, K.: *Kryptografie: Verfahren, Protokolle, Infrastrukturen.* Heidelberg: dpunkt.verlag 2013.

[6] BSI: *Leitfaden IT-Sicherheit.* Bundesamt für Sicherheit in der Informationstechnik (BSI) 2012.

[7] OWASP Foundation. (2019): *About The Open Web Application Security Project.* Retrieved from `https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project` (last access: August 27, 2019).

[8] OWASP Foundation. (2019): *OWASP Internet of Things Project.* Retrieved from `https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29` (last access: August 27, 2019).

[9] OWASP Foundation. (2019): *OWASP Internet of Things Project.* Retrieved from `https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10t` (last access: August 27, 2019).

[10] National Institute of Standards and Technology. (June, 2019): *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.* Retrieved from: `https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf` (last access: August 27, 2019).

[11] Department for Digital, Culture, Media and Sport: *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security.* Oct. 2018.

[12] Arias, O., Wurm, J., Hoang, K., Jin, Y.: *Privacy and Security in Internet of Things and Wearable Devices.* 2015.

[13] Kyas, O.: *How to Smart Home.* Key Concept Press 2015.

[14] Europäischen Union: *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES* - Datenschutzgrundverordnung 2016.

[15] Schwarz, F.: *Security and Privacy Investigation of Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices* Bachelor Thesis, Department of Informatics and Media, Technische Hochschule Brandenburg 2019.

[16] Schwarz, F., Schwarz, K., Creutzburg, R.: *Security and Privacy Investigation of Wi-Fi Connected and App-Controlled IoT-Based Consumer Market Smart Light Bulbs.* IS&T International Symposium on Electronic Imaging 2020, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2020, Society for Imaging Science and Technology, San Francisco (USA), Jan. 2020

Author Biography

Franziska Schwarz received her B.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2019. Since 2019 she is working as scientific assistant in Technische Hochschule Brandenburg. Her research work is focused on IoT and Smart Home Security.

Klaus Schwarz received his B. Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017. He is finishing his Master Thesis in 2020 and his research interests include IoT and Smart Home security, Embedded Systems, Artificial Intelligence, and Cloud Security.

Reiner Creutzburg is a retired professor for Applied Informatics at the Technische Hochschule Brandenburg in Brandenburg, Germany. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence, Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

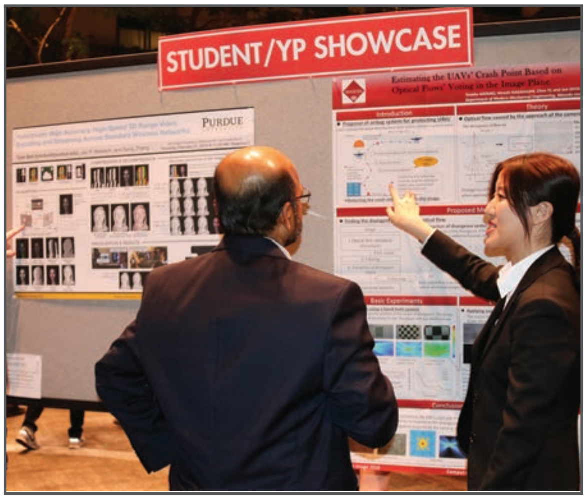
JOIN US AT THE NEXT EI!

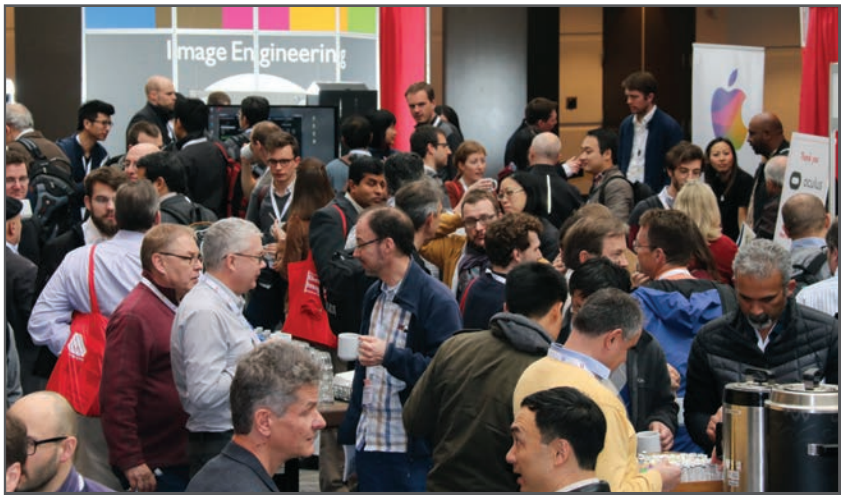
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





AR is a fundamental and transformative interface and platform.

20+ years from my initial working demo to today's AR displays

Optimistic that it won't take another 20 to reach ubiquitous consumer AR!

• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org