https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-275
© 2020, Society for Imaging Science and Technology

Security and Privacy Investigation of Wi-Fi Connected and App-Controlled IoT-Based Consumer Market Smart Light Bulbs

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

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 other devices is causing a rapid increase of vulnerabilities. Also, there are several vulnerabilities in software and hardware that make the security situation more complex and troublesome. Many of these systems and devices also process personal or secret data and control critical industrial processes. The need for security is extremely high. Owners and administrators of modern IoT devices are often overwhelmed with the task of securing their systems. Today, the spectrum of Smart Home technologies is growing faster than security can be guaranteed. Unsecured vulnerabilities endanger the security and privacy of consumers.

This paper aims to examine the security and privacy aspects of Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices. For this purpose, the communication between the device, app, and the manufacturer's servers, as well as the firmware of the individual devices, will be examined. In particular, this paper highlights why it is important to make consumers aware of the security and privacy aspects of Smart Home devices. Finally, it will be shown which dangers exist when using these devices, how the use of these devices affects the privacy and security of the device and its users, and whether the devices comply with the European General Data Protection Regulation.

Introduction

After the age of industrialization, a few things have changed the world as much as the Internet. After its beginning on October 29, 1969, when it was still called ARPANET, it has undergone many evolutions and triggered even more revolutions. The Internet has not only connected the world and created the "global village", but it has also brought us devices that change and shape society, such as the smartphone, which would not be what it is without the Internet. In addition to the many positive achievements associated with the Internet, it also brought the cyberwar - a new global battlefield as well as cybercrime, botnets and other threats and security concerns.[50] Now that the Internet has conquered the home computer from the net for mainframes and universities and has reinvented itself evolutionary in Web 2.0 with collaborative elements and social media, society is currently experiencing a further evolutionary stage of the World Wide Web – The Internet of Things (IoT). "Data has turned out to be the currency of the gigantic online companies, and so it is no wonder that relevant information collected from the smallest devices in the real world finds its way from the Internet of Things into the World Wide Web in real-time" [51]. These data collecting and sending devices are indeed so "small" and "inconspicuous", that although current studies show that there are already about 26 billion of them, "privacy and security concerns are only gradually emerging" [51]. As if that were not enough, the numbers are expected to triple again in the next five to six years, as shown in figure 1.

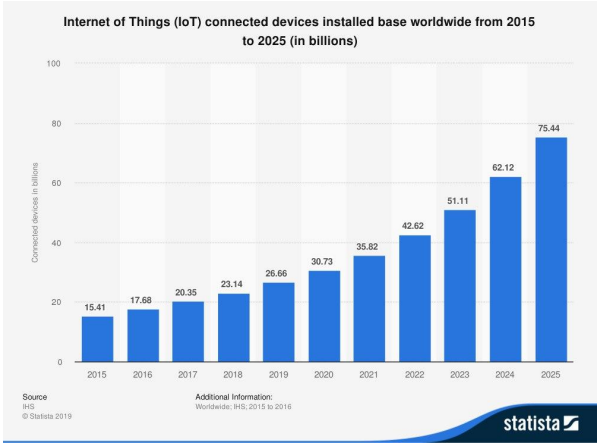


Figure 1. *IHS. "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions)". (2019): Statista. Web. Aug 20, 2019*

In a rapidly evolving market, privacy and cybersecurity considerations often fall off the table at high speeds, as new companies continue to bring new products to the market. This work aims to show the current state of security and privacy in a Security and Privacy Investigation of Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices.

Internet of Things

Internet of Things is generally a collective term for the networking of technologies. Under this term, technologies are collected that enable the networking of various elements from different areas in global infrastructure and thus allow them to work together. The Internet of Things, as a term in this paper, describes

the linking of clearly identifiable physical objects (things) as virtual representation on the Internet, a network similar to or equal to the Internet [2].

Smart Home

As in the previous definitions, the term Smart Home is a collective term. The term Smart Home thus refers to technical processes and systems in living spaces and houses (Home) whose main task is to improve the quality of life [46]. In this sense, the term Smart Home is defined in this paper. It is synonymous with devices that are intended for the living space of a human being and enable tasks such as the efficient use of energy, the networking of components of everyday life in the household, or even their remote control.

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 data security [40].

Device Security

Device security is about protecting a device from being used for an unintended or negative 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 [41].

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. [14].

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 private space 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 individuals concerning the processing of their data should ensure that their fundamental rights and freedoms, and in particular their right to protection of personal data, are respected irrespective of their 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.

Analysis Tools

This section introduces the analysis tools used. The tools are roughly divided into two categories. On the one hand, these are the tools for analyzing the firmware of the device, i.e., serial bootloader utility, disassembler, utility, and hex editor. On the other hand, network analysis, monitoring tools, and utilities to enable man-in-the-middle attacks.

esptool.py

The program esptool.py is "A Python-based, open-source, platform-independent, utility to communicate with the ROM bootloader in Espressif ESP8266 & ESP32 chips" [20]. The serial bootloader utility was initially developed by Fredrik Ahlberg as an unofficial community project and is now officially supported by the manufacturer Espressif. The Python-based program esptool.py is free software and certified under the GPLv2 license [20].

In this paper, the program esptool.py is used to create firmware dumps from the investigated devices. A firmware dump is an image of the internal memory of a device. Since all devices investigated in this paper using a chip from the same manufacturer, only this one program was used to read out the firmware. It is possible to destroy a fuse bit in the chip that prevents the firmware from being readout. Be that as it may, no manufacturer of the devices considered in this paper made use of it.

esp-bin2elf

The software esp-bin2elf is another Python-based program. It has the ability to convert flash dumps from Espressiv esp8266 based microcontroller to ELF executable [21]. The Executable and Linking Format (ELF) is a standard binary format from the UNIX world. Due to its wide distribution, several disassemblers support it. The program esp-bin2elf tries to map the sections found in the dump file to known sections of the ELF format and

includes all known SDK symbols. This makes disassembling the dump much easier, and many libraries can be easily recognized. In the context of this paper, the software is used for this very purpose. For example, complete images of the program sequence of individual devices could be created.

Radare2

The Radare2 software is a portable reverse engineering framework with the following capabilities [22]:

- Disassemble (and assemble for) many different architectures,
- Debug with local native and remote debuggers (gdb, rap, webui, r2pipe, winedbg, windbg),
- Run on Linux, *BSD, Windows, OSX, Android, iOS, Solaris and Haiku,
- Perform forensics on filesystems and data carving,
- Be scripted in Python, Javascript, Go and more,
- Support collaborative analysis using the embedded webserver,
- Visualize data structures of several file types,
- Patch programs to uncover new features or fix vulnerabilities,
- Use powerful analysis capabilities to speed up reversing,
- Aid in software exploitation.

It is used to disassemble the contents of the memory of the researched devices stored in binary format. In this investigation, it was possible to find out how the devices work, what the stored endpoints look like, and which data is stored on the device.

Ghex

As the name suggests, the software Ghex is a hex editor. This editor can open binary files and output their contents in Hex or ASCII. At the same time, the editor also allows adjusting the content of such files [23].

In the context of this paper, the editor was used to examine the memory content in detail, and to manipulate devices in an attempt to display them in the provider cloud in their developer account.

ISC DHCP, iptables and hostapd

The programs isc_dhcp_server, iptables, and hostapd were also used. They were used to set up a Wi-Fi hotspot, with which the communication of the registered devices can be intercepted in a Man-in-the-Middle attack. In this way, the endpoints of the individual devices could be determined. Besides, one can intercept how the devices communicate with the respective app as well as the communication of the app itself with the various clouds.

The website of the ISC DHCP software provides the following information about the program:

"ISC DHCP offers a complete open source solution for implementing DHCP servers, relay agents, and clients. ISC DHCP supports both IPv4 and IPv6 and is suitable for use in high-volume and high-reliability applications. DHCP is available for free download under the terms of the MPL 2.0 license" [24].

The Host Access Point Daemon or short hostapd is a daemon software that allows a network interface to act as an authentication server.

The software iptables is used to configure the tables provided by the firewall in the Linux kernel. These tables contain chains and rules such as PREROUTING, FORWARD, and POSTROUTING that are used as part of this paper to direct traffic through the man-in-the-middle proxy.

mitmproxy

The mitmproxy software is an HTTPS proxy that is free and open source. The interactive HTTPS proxy consists of three programs [25]:

- **mitmproxy** is an interactive man-in-the-middle proxy for HTTP and HTTPS with a console interface.
- **mitmdump** is the command-line version of mitmproxy. Think tcpdump for HTTP.
- **mitmweb** is a web-based interface for mitmproxy.

The software also offers the following features [25]:

- Intercept HTTP & HTTPS requests and responses and modify them on the fly,
- Save complete HTTP conversations for later replay and analysis,
- Replay the client-side of an HTTP conversation,
- Replay HTTP responses of a previously recorded server,
- Reverse proxy mode to forward traffic to a specified server,
- Transparent proxy mode on OSX and Linux,
- Make scripted changes to HTTP traffic using Python,
- SSL/TLS certificates for interception are generated on the fly,

Within the scope of this paper, the software is used to take a closer look at the data sent by the app via HTTPS. For example, keys for encrypted communication with the device could be intercepted.

darkstat

Darkstat is a software that records and uses network traffic to generate statistics of traffic-causing clients. These statistics can also be retrieved in a web interface.

The website of the software lists the following features [26]:

- Traffic graphs, reports per host, shows ports for each host,
- Embedded web-server with deflate compression,
- Asynchronous reverse DNS resolution using a child process,
- Small, Portable, Single-threaded, Efficient,
- Supports IPv6.

As part of this paper, the darkstat program is used to obtain accurate statistics on the Internet use of individual devices. These statistics allow, among other things, comprehensive insights into which ports the researched devices open and which endpoints are communicated with (fig. 3).

tuyadump

The program tuyadump helps to extract the communication from Tuya devices. Tuya is a supplier and service provider of microcontrollers, which, in combination with various devices from different manufacturers, meet the Smart Home Definition of this paper. The program was used to provide information about the

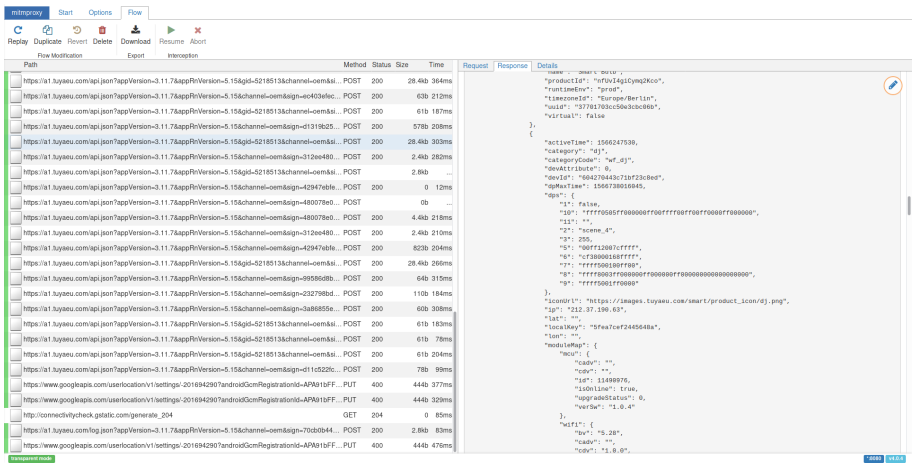
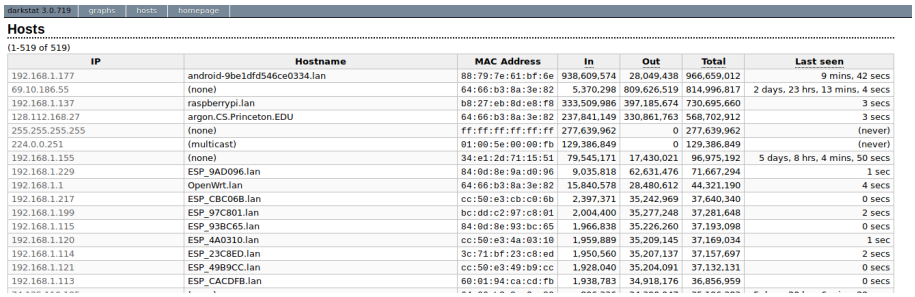


Figure 2. *mitmproxy – Traffic Inspection*



darkstat 3.0.719 | graphs | hosts | homepage

Hosts

(1-519 of 519)

IP	Hostname	MAC Address	In	Out	Total	Last seen
192.168.1.177	android-9be1dfd546ce0334.lan	88:79:7e:61:bf:6e	938,609,574	28,049,438	966,659,012	9 mins, 42 secs
69.10.186.55	(none)	64:66:b3:8a:3e:82	5,370,298	809,626,519	814,996,817	2 days, 23 hrs, 13 mins, 4 secs
192.168.1.137	raspberrypi.lan	b8:27:eb:8d:e8:f8	333,509,986	397,185,674	730,695,660	3 secs
128.112.168.27	argon.CS.Princeton.EDU	64:66:b3:8a:3e:82	237,841,149	330,861,763	568,702,912	3 secs
255.255.255.255	(none)	ff:ff:ff:ff:ff:ff	277,639,962	0	277,639,962	(never)
224.0.0.251	(multicast)	01:00:5e:00:00:fb	129,386,849	0	129,386,849	(never)
192.168.1.155	(none)	34:e1:2d:71:15:51	79,545,171	17,430,021	96,975,192	5 days, 8 hrs, 4 mins, 50 secs
192.168.1.229	ESP_9AD096.lan	84:0d:8e:9a:d0:96	9,035,818	62,631,476	71,667,294	1 sec
192.168.1.1	OpenWrt.lan	64:66:b3:8a:3e:82	15,840,578	28,480,612	44,321,190	4 secs
192.168.1.217	ESP_CBC06B.lan	cc:50:e3:cb:c0:6b	2,397,371	35,242,969	37,640,340	0 secs
192.168.1.199	ESP_97C801.lan	bc:dd:c2:97:c8:01	2,004,400	35,277,248	37,281,648	2 secs
192.168.1.115	ESP_93BC65.lan	84:0d:8e:93:bc:65	1,966,838	35,226,260	37,193,098	0 secs
192.168.1.120	ESP_4A031D.lan	cc:50:e3:4a:03:10	1,959,889	35,209,145	37,169,034	1 sec
192.168.1.114	ESP_23C8ED.lan	3c:71:bf:23:c8:ed	1,950,560	35,207,137	37,157,697	2 secs
192.168.1.121	ESP_49B9CC.lan	cc:50:e3:49:b9:cc	1,928,040	35,204,091	37,132,131	0 secs
192.168.1.113	ESP_CACDFB.lan	60:01:94:ca:cd:fb	1,938,783	34,918,176	36,856,959	0 secs

Figure 3. *darkstat – Hosts Overview*

communication characteristics of some of the devices. Among other things, this program could help to understand the encryption used by these devices.

Princeton IoT Inspector

Princeton IoT Inspector is a desktop tool that attempts to monitor IoT devices to help identify privacy and security issues. The data collected is shared with researchers from Princeton University in the USA. Monitoring IoT devices with this program, therefore, has the dual benefit of being relatively easy to keep track of on the one hand devices in the home and, on the other hand helping to conduct a valuable study aimed at getting an overall view of problems, privacy, and security [27].

This paper uses this software to set up a long-term monitoring system that is easy to replicate for other consumers and provides practical and reliable results. The Princeton IoT Inspector provides valuable real-time information for this purpose and can be configured to send a warning if there is any indication that a safety incident has occurred.

Wireshark

Wireshark is a so-called sniffer. It helps with the preparation and evaluation of data protocols. It is used for network troubleshooting, analysis, development of software and communication protocols, and training. Wireshark is free and open-source. The software is available for several different platforms and offers a graphical user interface.

The software is used in the context of this paper for the evaluation of network traffic. The Smart Home devices researched in this paper use a wide variety of protocols and sometimes communicate unencrypted. Here, the software was used to be able to trace the relevant data traffic in a targeted manner.

Security and Privacy Investigation

The market for IoT devices is almost infinitely large. With more than 26 billion devices in circulation and a forecast of tripling this number over the next five to six years, there are countless new vendors every day. As part of this work, ten IoT-Based Smart Home devices, including light bulbs, sockets, and a relay, were investigated in terms of security and privacy. The manufacturers of these devices are colorfully mixed, partly known, or even completely unknown. They were bought in a DIY store, an electronics retailer, and on the internet. The prices are all low, and it is essential to note that these devices are not only entry into new technology and thus into a new age of the internet, but also complex computer systems. To study these devices, it required clear objectives, a sophisticated laboratory environment, and a checklist of thirty-one pages and 168 questions.

Investigated IoT Devices

The following devices were investigated:

- EDNET 84336 Voice-Controlled Wi-Fi Power Socket
- Bawoo Wi-Fi Smart Light Bulb
- Mpow Smart Wi-Fi Lampe
- Luminea Home Control Wi-Fi Light Bulb
- Hama Wi-Fi Power Socket

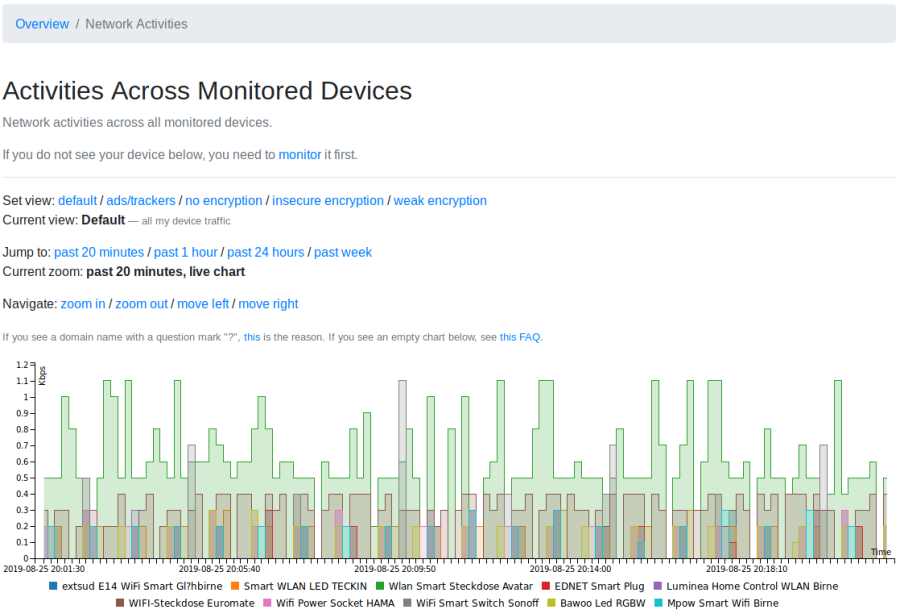


Figure 4. *Princeton IoT Inspector – Traffic Overview*

- Wi-Fi Stecker Schuko Schwarz
- Smart Wi-Fi LED TECKIN
- Wi-Fi Smart Switch Sonoff
- extsud E14 Wi-Fi Smart Light Bulb
- Wi-Fi Smart Power Socket Avatar

Technical Details:

- Voice-operated power outlet for Google Home and Amazon Alexa
- Complies with Wi-Fi IEEE standard IEEE802.11b/g/n
- Frequency range: 2.412 ˜2.484 GHz
- Compatible with Android & iOS
- Input voltage: AC 85 ˜265 V, 50 Hz
- Item Lamp socket: E27, Illumination type LED (RGBW)
- Output current: 10 A (max.)
- Voltage: 230 V, max. 2300 W
- Power Rating: 3680 W
- LED status indicator, Timing Function
- Lifetime 30000-35000 hours
- FCC, CE and IFTTT approved
- Energy efficiency class A+/A++
- Weight: 9 g - 159 g
- Operation with 2.4 GHz Wi-Fi router
- Light output: 650 - 800 Lumen

Objectives of the investigation

The objectives of the investigation lie with the title of the work clearly defined. The tested devices shall be researched for their security and privacy characteristics, as defined in this paper. Security is in general freedom or resistance to potential damage and the absence of unjustifiable risks. These characteristics are to be investigated because of the Device Security as well as the Data Security. We investigated whether and how a device is protected from being used for an unintended or negative purpose. Besides, we considered the implementation of the protection of the technical processing of information. Besides, it is important to check the compliance of manufacturers, cloud providers, and devices with the security aspects. On the privacy side, it is particularly important to check compliance with the right to privacy, which is a general human right.

Security and Privacy Checklist

To guarantee compliance with the stated objectives and to ensure consistent quality, a questionnaire was developed in connection with the Smart Home Security and Privacy Evaluation Cycle presented in [53] and [54]. The Security and Privacy Checklist for Wi-Fi Connected and App-Controlled IoT-Based Smart Home Devices comprises thirty-one pages and over 160 questions on all stages of the Smart Home Device life cycle. The checklist is also designed for amateurs and attempts to make the risks to privacy and security known at every step of the life cycle. A short and beneficial version of this checklist is given in the appendix of [54].

Laboratory Environment

A complex laboratory environment had to be created for the devices to be examined within the scope of this paper. To research the devices concerning their safety and the protection of privacy, this laboratory is divided into two parts. On the one hand, there is the firmware side. For this, the devices were partially physically destroyed and opened to read the existing data. On the other hand, there is the Network side where data is analyzed how, with whom, in which way and in which frequency the Smart Home devices communicate. First, the structure of the environment for analyzing the firmware will be shown.

The analysis tools described in section were used to examine the firmware. First, the devices were individually inspected and researched for their properties. The devices were then opened for

firmware analysis (fig. 5). It had to be determined what kind of microcontroller it was and where on the chip the serial interface was led out. Then the serial interface was soldered with cable extensions (fig. 6) to facilitate the reading of the firmware. After the correct connection of the pins RX (Receiver), TX (Transmitter), and Ground, the microcontroller could be connected to an external power supply with 3.3 V DC voltage. To read the firmware, one has to boot into the debug mode. This can be achieved by switching the debug pin GPIO0 to the ground.

Figure 5. *Before and After Opening*

Figure 6. *Microcontroller with Soldered Extensions*

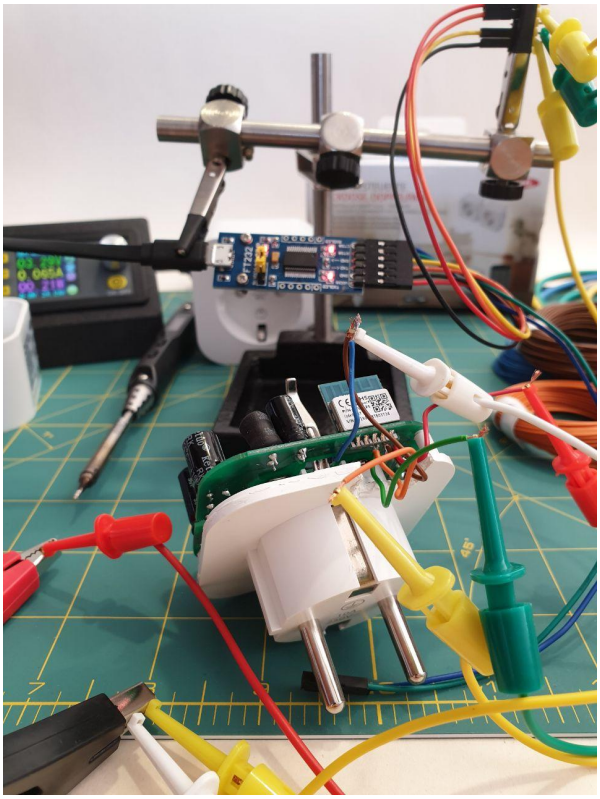


Figure 7. *Firmware Dumping Process*

The program esptool.py is used to read the memory on the microcontroller (fig. 7). After a successful reading, the binary can be viewed in the hex editor (fig. 8) and must be converted into an ELF executable with the help of esp-bin2elf. After a successful conversion, the firmware image can be researched in the disassembler (fig. 9).

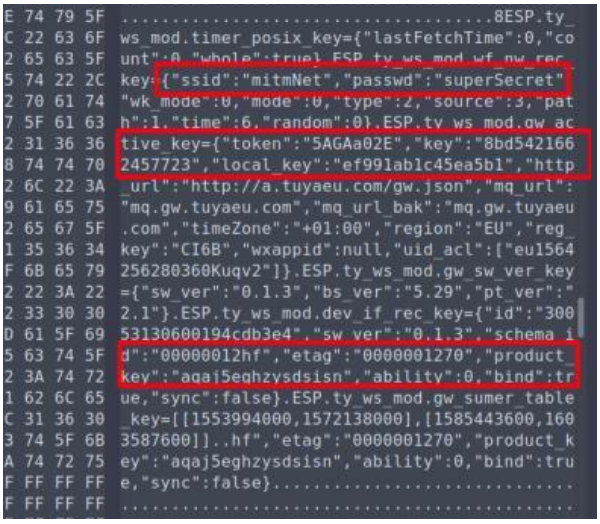


Figure 8. *Private Data in the Device Memory*

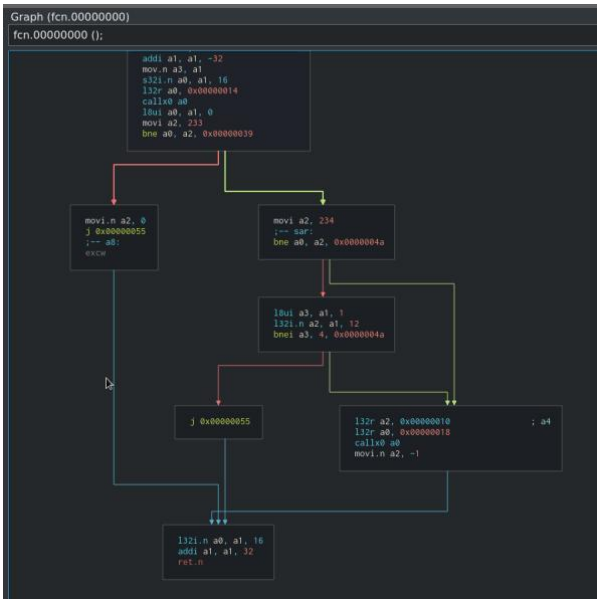
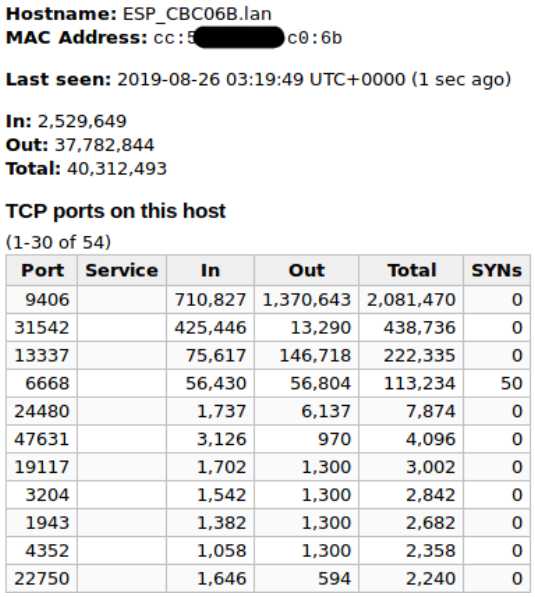


Figure 9. *Program Sequence of the Boot Loader*

On the network side, a Wi-Fi access point was first set up with the tools ISC DHCP and hostapd. With the help of the iptables program, traffic is redirected so that a man-in-the-middle attack can be carried out with the mitmproxy software. To listen to encrypted HTTPS traffic, the mitmproxy program issued a certificate and set it up on the laboratory smartphone. From now on, the entire traffic of the app could be viewed in the web interface of the software mitmproxy (fig. 10, 12). In addition to the mitmproxy program, the darkstat software was installed on the router to obtain statistics on traffic and open ports (fig. 11). On the device side, the data was evaluated using the tuyadump and Wireshark programs.

Figure 10. *Keys and IDs Inside App Traffic*



Hostname: ESP_CBC06B.lan
MAC Address: cc:5[redacted]c0:6b

Last seen: 2019-08-26 03:19:49 UTC+0000 (1 sec ago)

In: 2,529,649
Out: 37,782,844
Total: 40,312,493

TCP ports on this host

(1-30 of 54)

Port	Service	In	Out	Total	SYNs
9406		710,827	1,370,643	2,081,470	0
31542		425,446	13,290	438,736	0
13337		75,617	146,718	222,335	0
6668		56,430	56,804	113,234	50
24480		1,737	6,137	7,874	0
47631		3,126	970	4,096	0
19117		1,702	1,300	3,002	0
3204		1,542	1,300	2,842	0
1943		1,382	1,300	2,682	0
4352		1,058	1,300	2,358	0
22750		1,646	594	2,240	0

Figure 11. *Opened Ports on a Device*

Figure 12. *Exposed Location Inside App Traffic*

The Princeton IoT Inspector was also installed to enable long-term monitoring. It runs on one side in the local network and tries to detect the existing Internet of Things devices and sends the detected data to a server in Princeton for evaluation. The statistics generated there look like this (fig. 13).

Evaluation – The Good – The Bad – The Ugly

A unique identity, the ability to communicate wirelessly and either a sensor or an actuator, more it does not need, and a simple thing is in the Internet of Things. According to the study from figure 1, there are already 26.6 billion pieces of these things on the internet of things. A big market and an exciting and promising business opportunity. As the same study in Figure 1 shows, the number of these things on the Internet should triple from 26 billion to over 75 billion in the next five to six years.

This paper revolves around security and privacy in conjunction with IoT-Based Smart Home devices. The **good** side about these devices is they are much fun. They make the daily routine easier; they are easy to set up, are always connected, and getting started is not particularly expensive. The Internet of Things is growing, and that is good because it is its most significant potential. According to the study in Figure 1, there are already five billion more devices of this kind in the coming year. In a market with so much movement and so many competitors, those who deliver quality can assert themselves better. IoT based Smart Home devices, unlike Smart Phones, which only differ in the number of cameras, still has the chance of real innovation. In the next five years, there will be more than ten times as many IoT devices as people in the world, and that is the best thing that can happen to the Smart Home and, at the same time, its most significant chance.

The **bad** side about the Smart Home is clearly the lack of standards as already described, the Internet of Things is developing explosively, and so it is no wonder that in this rapid development, there is pure chaos as far as the standards of the devices are concerned. All devices tested in the course of the paper communicated mainly via the MQTT protocol. The most diverse implementations of control codes and ports have made the work of investigation and the work of the community difficult. Different peculiarities such as port knocking mechanisms where a specific sequence has to be called on different ports during connection setup have made the investigation even more difficult. Besides, the ten tested devices need three different Apps. The cooperation of different manufacturers is simply not given. If devices from different manufacturers are installed within a home, all providers have almost the same amount of private data. The different standards, the lack of cooperation, and the many peculiarities are the bad thing about the Smart Home and the whole Internet of Things.

The **ugly** side of the Internet of Things is the more precarious situation in terms of privacy and security. The market is growing so fast that there simply does not seem to be time for sufficient security implementations. So it happens that none of the tested devices require a strong password for authentication. What is worse is that the devices can often be dismantled and read without leaving a trace. Keys and Ids for encrypted communication with the cloud are stored unencrypted in the memory of the devices, just like the credentials for the local Wi-Fi. A sixteen digit code from memory is usually sufficient to listen to the entire communication. The worst thing, however, is that updates are neither transmitted via HTTPS nor signed. So it is possible to flash a modified firmware with the keys that can also be intercepted in the communication with the app. For home users with interest in this area, there is not only a proof of concept but even a ready-to-use solution, which the company VTRUST GmbH and the German tech magazine c't have developed together and keep up to date. Protective measures concerning privacy are simply not

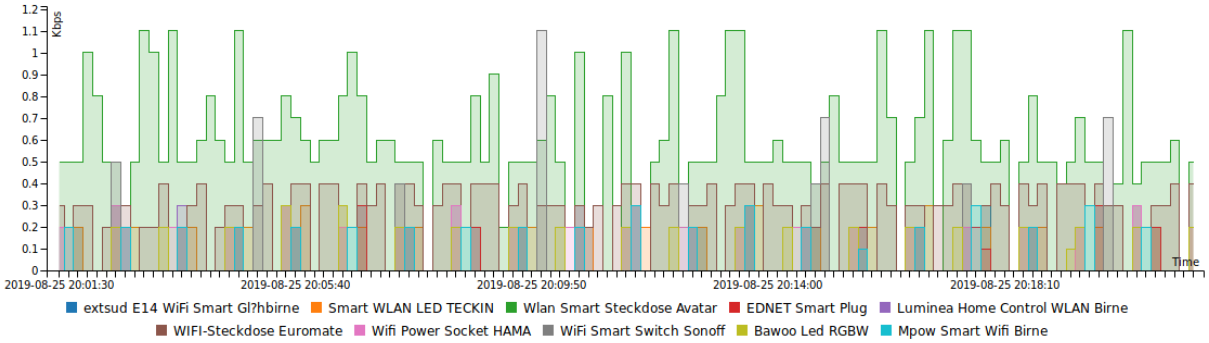


Figure 13. *Traffic Statistics of the IoT Devices*

included. Even in the case of well-known products, only negative aspects could be identified in the context of this paper. Most manufacturers wrote on the subject of the privacy policy that the policy of the cloud provider had to be consolidated, while the cloud provider wrote that the topic was the responsibility of the manufacturers — no Privacy by Design and by Default at all [44]. One app could even only be launched after it had viewed the current location. These apps communicate real-time location data, usage statistics, and other private data collected by individual devices without any asking.

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.

References

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

[2] Tripathy, B., Anuradha, J.: *Internet of Things (IoT): Technologies, Applications, Challenges and Solutions* Taylor & Francis Ltd 2017.

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

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

[16] 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).

[17] 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).

[18] 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).

[19] 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).

[20] esptool Software Description, `https://github.com/espressif/esptool` (last access: August 27, 2019).

[21] esp-bin2elf Software Description, `https://github.com/jsandin/esp-bin2elf` (last access: August 27, 2019).

[22] Radare2 Software Description, `https://rada.re/r/` (last access: August 27, 2019).

[23] Ghex Software Description, `https://wiki.gnome.org/Apps/Ghex` (last access: August 27, 2019).

[24] dhcp-server Software Description, `https://www.isc.org/dhcp/` (last access: August 27, 2019).

[25] mitmproxy Software Description, `https://docs.mitmproxy.org/stable/` (last access: August 27, 2019).

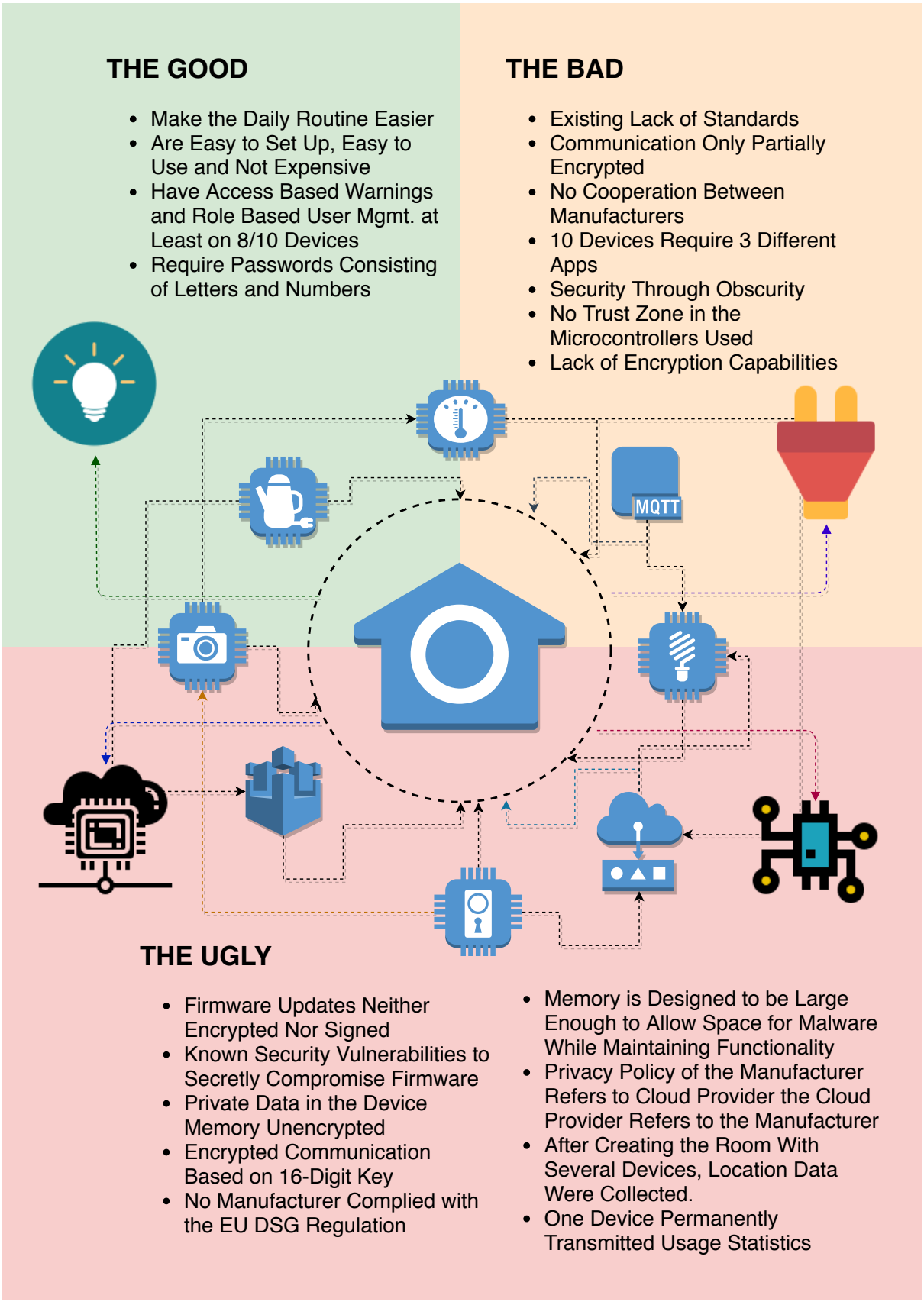


Figure 14. *Evaluation — The Good – The Bad – The Ugly*

[26] darkstat Software Description, https://unix4lyfe.org/darkstat/ (last access: August 27, 2019).
[27] iot-inspector Software Description, https://iot-inspector.princeton.edu/blog/post/faq/ (last access: August 27, 2019).
[40] 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.
[41] Arias, O., Wurm, J., Hoang, K., Jin, Y.: *Privacy and Security in Internet of Things and Wearable Devices.* 2015.
[42] Wireshark: *Wireshark - About* The Wireshark Foundation, 2018.
[43] Portswigger Software Description, https://portswigger.net/about (last access: August 27, 2019).
[44] Hu, F.: *Security and Privacy in Internet of Things (IoT) - Models, Algorithms, and Implementations.* CRC Press 2016.
[45] Dehghantanha, A., Choo, K.-K. R.: *Handbook of Big Data and IoT Security.* Springer 2019.
[46] Al-Qutayri, M. A.: *Smart Home Systems.* In-Tech 2010.
[47] Kyas, O.: *How to Smart Home.* Key Concept Press 2015.
[48] Zhu, L., Zhang, Z., Xu, C.: *Secure and Privacy-Preserving Data Communication in Internet of Things.* Springer 2017.
[50] Bunz, M.: *Vom Speicher zum Verteiler. Die Geschichte des Internet* 2008.
[51] Lea, P: *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security* Packt Publishing 2008.
[52] Europäischen Union: *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES* - Datenschutzgrundverordnung 2016.
[53] 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.
[54] Schwarz, F., Schwarz, K., Creutzburg, R.: *New Methodology and Checklist of Wi-Fi Connected and App-Controlled IoT-Based Consumer Market Smart Home Devices.* 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 is a M.Sc. student of Computer Science at Technische Hochschule Brandenburg (Germany). She received her B.Sc. in 2019 and is working as a 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.

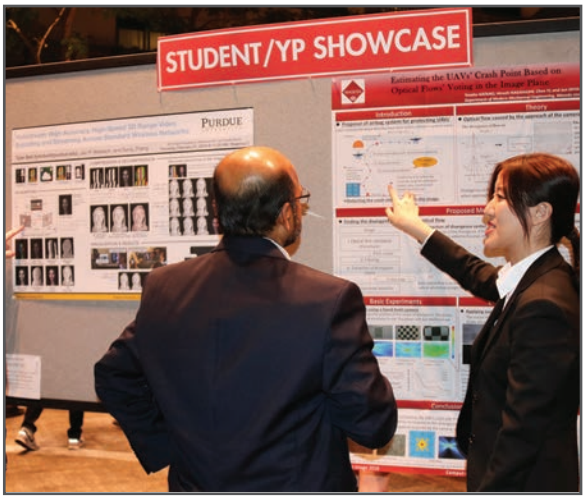
JOIN US AT THE NEXT EI!

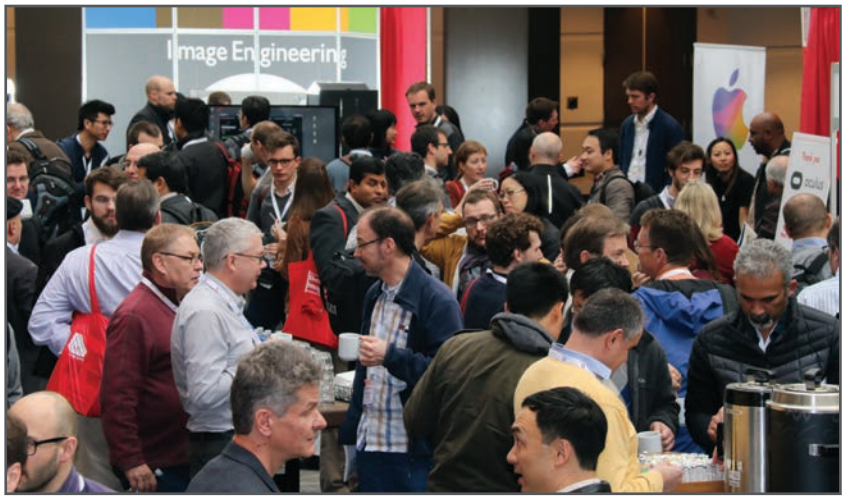
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

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





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

www.electronicimaging.org

IS&T
imaging.org