https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-277

Conception and implementation of a course for professional training and education in the field of IoT and smart home security

Michael Pilgermann, Thomas Bocklisch, Reiner Creutzburg

Technische Hochschule Brandenburg, Department of Informatics and Media, IoT and Smart Home Security Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany

Email: michael.pilgermann@th-brandenburg.de, bocklisch@th-brandenburg.de, creutzburg@th-brandenburg.de

Abstract

The aim of this paper is to describe the new concept of a Master level university course for computer science students to address the issues of IoT and Smart Home Security. This concept is well suited for professional training for interested customers and allows the creation of practical exercises.

The modular structure of the course contains lectures and exercises on the following topics:

1. *Introduction - IoT and Smart Home Technology and Impact*
2. *Homematic Technology and Smart Home Applications*
3. *Loxone Technology and Smart Home Applications*
4. *Raspberry Pi and Smart Home Applications*
5. *Security of IoT and Smart Home Systems*

and contains laboratory exercises of diverse complexities.

Introduction

The rapid growth of the Internet of Things and its networked devices has led to exponential data growth with the goal of making devices smarter, processes more efficient, and life easier overall. This massive generation and collection of data has its advantages, but easy access to data also has increased vulnerabilities - unsecured IoT devices pose a serious risk to personal and business information.

Securing IoT devices is a challenge for several reasons. A rapidly growing number of gadgets are becoming smart devices, and as manufacturers launch new products faster, security will often be given a low priority as the focus is on time-to-market and return-on-investment efforts. Lack of consumer and business awareness is also a major security barrier as the convenience and cost savings benefits of IoT technology seem to outweigh the potential risks of data breaches or device hacking.

To respond to these issues professionally, it is important to have well trained staff. The fact that many agencies and companies work with very sensitive data makes it necessary to further train their own employees in the field of IoT and Smart Home Security. Moreover, further penetration of the market with those products will result in higher overall dependency on those products and connected services.

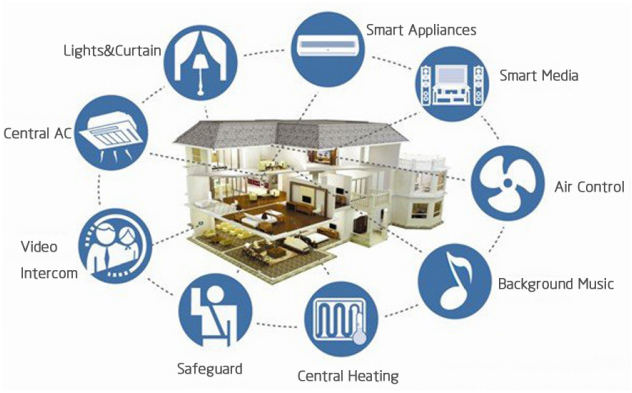


Figure 1. *Smart Home - Overview on selected functionalities (image src: `http://www.ohsungec.com/`)*

Conception

In the following, the concept of the IoT security traineeships will be presented. The section will show the general method and the structure of the traineeship. The structure is the same for all subtasks. Furthermore, basic information about hardware and software are given because certain techniques and procedures must be applied independently of the task.

General conditions

The *Brandenburg University of Applied Sciences* offers different Computer Science courses of studies, in which this module is integrated. Several BSc grade courses allow students for focusing on health informatics or multimedia issues. A BSc in any kind of Computer Science course is a prerequsite for subscribing to this IoT module.

The module *IoT and Smarthome Security* is an elective module within the Master of Science (MSc) courses in Computer Science at the Brandenburg University of Applied Sciences. Usually it shall be taken in the second term of the MSc course [8]. Students achieve six credits when passing the module. Neither the BSc modules nor the MSc modules at the Brandenburg University of Applied Sciences had provided any explicit previous knowledge regarding Internet of Things or Smart Home technologies.

The university has a history with similar modules. Experiences from an equivalent module for experiments in a forensic lab have been reported in [7].

Objectives of course

The following objectives were codified when formally defining the module:

- Once the students have successfully passed the module, they can name security challenges in existing IoT- and Smart Home applications as well as forecast those challenges for future installations.
- The students can apply IoT- as well as Smart Home tailored implementations of security protocols.
- The students are able to deploy methodology when drafting and utilizing security systems and protocols for IoT- and Smart Home installations.
- The students can analyze existing procedures and technologies, can estimate their security risks and can suggest appropriate security controls.
- The students can perform non-complex penetration tests on IoT systems.
- The students discuss the impacts of security concepts regarding complexity of IT systems and levels of security.

Lab environment

Thanks to the financial support of the European Regional Development Fund (ERDF) [9] a laboratory at Brandenburg University of Applied Science was equipped with state of the art IoT and primarily Smart Home products and solutions. The following product groups were deployed by the engineering staff of the university and are the base for the exercises:

- Loxone products: three mobile demo cases (see figure 2) and one permanent deployment with several sensors and actors inkl. alarm sirene
- Base for open source deployments: 4 kits based on Raspberry Pi 3
- Homeatic CCU3 Homeserver and several sensors
- Lighting and other gadgets: Phillips Hue, Bosch, Fibaro and Eve components
- Voice interaction: One Alexa
- Network equipment: LAN / VAN routers inkl. wireless routing as well as switches allowing for network penetration (esp. mirror ports)
- AVM products for home automation based on DECT standard

The components were all connected in an isolated network through the campus network of the Brandenburg University of Applied Sciences to the Internet. This way, students could also run experiments analyzing the network traffic home of IoT equipment.

Modules

As the module is defined as a hands-on module with focus on practical lab experiments, the theoretical part was to be kept as minimal as possible. However, due to the general lack of previous knowledge resulting from the study plan, some basics had to be introduced at the beginning of the term.

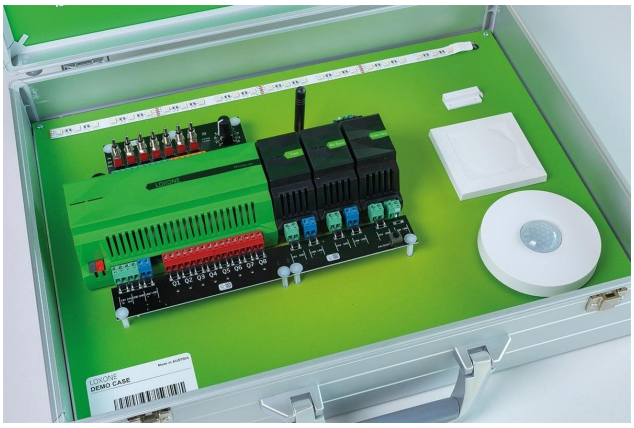


Figure 2. *Loxone Demo Case (image src: loxone.com)*

Three of those introductory presentations are explained in more detail as follows. Other topics such as Homematic systems and technology, open Smart Home systems based on Raspberry Pi or Software Defined Radio are as well part of the focus areas.

After those introductory presentations the students were asked to choose a focus topic. This focus was highly related to the experiment, they were carrying out (see following section for details).

Overview on IoT and Smart Home technology

Due to the curriculum of the courses the the Brandenburg University of Applied Sciences, the students came across the topics Internet of Things and Smart Home for the first time. Therefore an introduction gave an overview on the topic itself, the technological and economical impact of Internet of Things. IoT was also put into relation to other topics such as Industrial Control Systems (ICS) or Critical Infrastructure Protection. Students learnt about the relevance of the technology and the forecast, showing them about the expected growth (figure 3). Already at this point in time, the inter-connectivity was explicitly stressed, showing that IoT devices are ultimately connected (often to the Internet) and this way exposed to a waste number of threats from the Cyber space.

Loxone technology and smart home applications

The topics of the module made sure to integrate free and open source solutions as much as Enterprise or popular proprietary products in order to prepare students for the employment market. The Brandenburg University of Applied Sciencs had decided to integrate the Enterprise Smart Home solution of *Loxone* (`www.loxone.com`), an Austrian vendor, in their curriculum and their lab.

The lectures on Loxone gave first of all an overview of the solution with its components and user interface. More details were discussed on the configuration / programming paradigm, the API (web-service interface), the protocols (and their security attributes), remote access options to the installation and options for interfacing / integrating with other Smart Home solutions or approaches.

All students no matter what focus they chose afterwards were

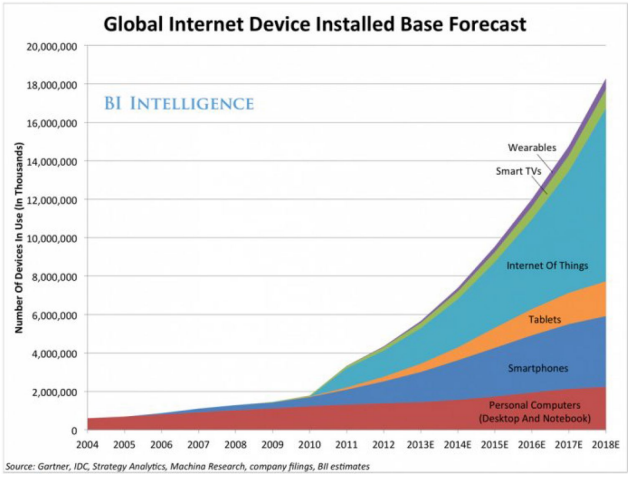


Figure 3. *Global Internet Device Installed Base Forecast (image src: Business Insider)*

at the end of this block requested to perform basic operations on the Loxone Miniserver and its peripheral devices.

Security deep-dive

The session is opened by a discussion of sample incidents on or weaknesses in Smart Home or Internet of things solutions in the past.

Vulnerabilities

2016: The challenges when remote accessing an Enterprise Smart Home solution through the Internet were discussed using an example from 2016. The vendor Loxone had combined two weaknesses making it easy for potential perpetrators to hack into the system: Firstly, the authentication for the privileged account was based on well documented default credentials, for which customers were not forced to change them. Secondly, the Loxone Dynamic DNS service *Loxone Cloud DNS* tailored for making Loxone installations easily accessible from the Internet was based on the MAC addresses of the Miniservers, which could easily be guessed due to their ascending order. Back in 2016, the researcher could have gained privileged access to 110 installations with very limited effort [13].

2016: Again in 2016 much of the Internet broke down for about a day caused by an attack on the servers of *Dyn*, a major upstream DNS provider (internet's domain name system (DNS)). The weapon for this attack was a Distributed Denial of Service attack, which was mainly orchestrated through the so called *Mirai* botnet (see figure 4 for global spread of Mirai bots) [14, 15]. This major attack is to be discussed from two perspectives regarding Internet of things:

- The bots in the Mirai network are mainly said to be Internet of Things devices. Due to the ever increasing connectivity of those devices nowadays, they can cause - when infected due to improper security controls - massive volumes of traffic.
- Architectures of modern IoT solutions often include Could services for providing the services to customers. A break down of central Internet services such as DNS does directly impact the functioning of those solutions as much as their functioning depends on a Cloud service.

Figure 4. *Mirai botnet behind Dyn DDOS attacks (image src: Softpedia News)*

2019: This example from 2019 illustrates the effect of the poisoning partnership of week security controls and Internet connectivity of IoT devices. For the *EmbedThis GoAhead* web server a critical code execution vulnerability (CVE-2019-5096) was reported through responsible disclosure. Even though the vendor of GoAhead professionally reacted and patched the software against the vulnerability, a waste number of IoT devices have been exposed through this vulnerability. This is due to the fact, that GoAhead designed to be a fully customizable web application framework and server, is widely used in IoT devices [16]. The devices can either not be updated or patched; vendors do not accept responsibility.

Basic security controls for IoT

Moreover, some basic security principles for users of smart homes were introduced. Fortunately, the Federal Office for Information Security, Germany (BSI) does provide some guidance on how to use Smart Home products [1]. This way, the following rules are the base for a discussion on state of the art security controls:

1. Consider security attributes of products *before* purchasing.
2. Change all default credentials immediately upon start-up.
3. Activate encryption, also for domestic connections.
4. Provide dedicated Internet Wireless LAN for your guests (not the same as for your Smart Home devices).
5. Question, very question the need for Internet connection of your IoT devices.
6. Use VPN for access to your IoT products from the Internet.
7. Network segmentation - use a dedicated Wireless LAN for your IoT devices.

Moreover, an introduction is given on how security can be designed, implemented and operated for Smart Home solutions. Approaches included here are mainly good practices from standardization bodies such as ETSI or DIN ([17, 18]).

Results from first run of exercises

The master course was carried out for the first time in summer term 2019 with about 15 students as a shared efforts between three lecturers.

The students had to choose one topic from the following list

Figure 5. *Comparison of wiring options for connecting peripheral devices to Miniserver*

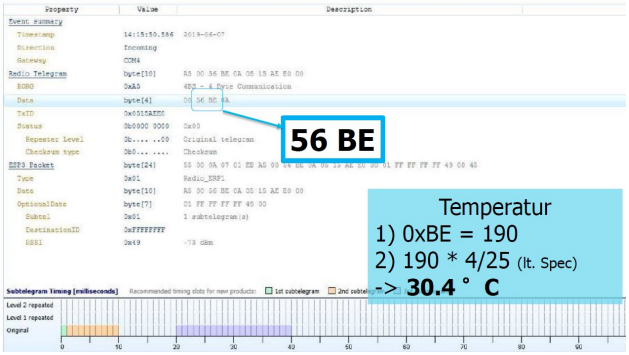


Figure 6. *Screenshot of Enocean Monitor for analyzing traffic*

for their experiments. The topics were prepared by the lectures to be handled by groups of 2 up to 3 students:

- Examination of security properties of wireless IoT protocol Enocean
- Secure access to Loxone API
- Examination of security properties of proprietary protocol Loxone Tree
- Monitoring and Intrusion Detection for Smart Home/ IoT networks with a Raspberry Pi
- Software-Defined Radio to analyze Smart Home/IoT systems
- Penetration Testing of Smart Home/IoT devices
- Application of OSINT technologies for tracing weaknesses in Smart Home devices
- Introduction in the handling of Censys and the Censys API
- Introduction in the handling of Maltego

The students generally had to do some literature / online research on the topic and - primarily - carry out practical tasks in the laboratory. In the end, they had to hand in a report on their topic. Additionally, a presentation on the topic, the experiments and the findings had to be given in a plenary session of all lecturers and students.

Three examples of exercises are presented in more details as follows.

Exercise 1: Evaluation Enocean

EnOcean is an energy harvesting wireless technology for Smart Homes. The EnOcean Alliance, which comprises about 250 companies, is in charge of agreeing upon profiles (EnOcean specifications), which allow for interoperability. Following the website and documentation, quite some efforts had been put on the security when shaping and improving the technology (so-called *Dolphin architecture*).

The students are tasked to analyse, how much security does really end up in the products and to what extend the security features are enabled. The following tasks are to be fulfilled by the students:

- Analyzing of the specification itself regarding its security architecture
- Develop and document a concrete lab setup
- Carry out and document several security relevant experiments
- Collect findings and mirror against good practice for Smart Home security
- Explicitly explore on the choices, the customers have got regarding security capabilities of the products.

The lab setup for the EnOcean experiment similar to [11] included a Loxone Miniserver with an EnOcean extension, a Windows 10 PC with an EnOcean USB Connector (so-called USB 300), a push button switch, a rocker for push button switch and a temperature sensor. On the software side EnOcean DolphinView and Loxone Config was provided for applying configurations and carrying out monitoring.

Findings

In theory the security features of EnOcean are comprehensible.

The software provided by EnOcean *DolphinView* does a good job in monitoring the EnOcean traffic at the corresponding frequencies. Figure 6 provides an example of that monitor, displaying the traffic captured at the Windows-10-PC (with USB 300) between the temperature sensor and the Loxone Miniserver.

Encryption is rarely supported by the products. For the push button switch it was even necessary to purchase additional hardware in order to enable customers to activate encryption. Coming back to the example from figure 6, the students shall consult the specification of Enocean ([12]) in order to gain the information communicated from the sensor to the Mini-Server (here air temperature).

Customer information is week and deceptive. The boxes for the products in the experiment were all decorated by key symbols indicating some kind of security and encryption. Furthermore, the products did not include any additional information on how to deal with security or at least on how to activate security features such as encryption.

Exercise 2: Open Source Intelligence

One major issue in IoT security is the combination of poor security with a high level of connectivity. Week login credentials or a lack of software updates become more severe problems as soon as those devices get connected to the Internet. Thanks to the cloud computing trend, we observe an ever increasing connectivity especially for IoT devices. Then often protection of those devices are based on *security by obscurity* - saying, not to find the device in the Internet. Security by obscurity is dead - this is even more the case for our concrete challenge in ḧidingḮoT devices.

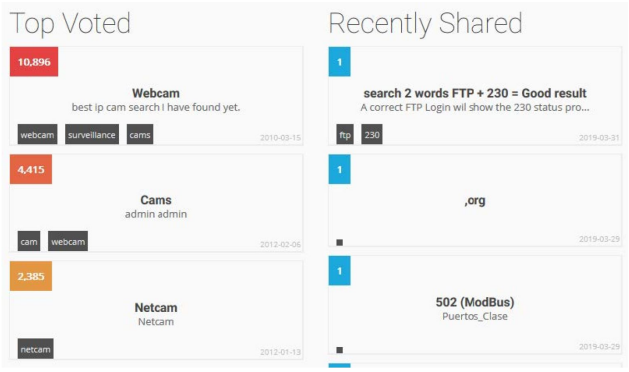


Figure 7. *Screenshot of Shodan website showing statistics (`https://www.shodan.io/explore`)*

In order to introduce this challenge to the students, an experiment on Open Source Intelligence [10] using the search engine *Shodan* (`www.shodan.io`) was set up. Shodan is said to be the most dangerous search engine on earth. Shodan attempts to assemble catalogues of meta information about its targets. Shodan often collects data on web servers (HTTP/HTTPS via ports 80, 8080, 443,8443), FTP (port 21), SSH (port 22), Telnet (port 23), SNMP (port 161), SIP (port 5060), and the Real Time Streaming Protocol (RTSP, port 554). RTSP is usually used for accessing web cams or video streams. Hackers as well as security researchers are using Shodan regularly for finding webcams, traffic lights, wind wheels, ICS systems or other IoT devices on the Internet.

The following tasks are part of the experiment:

- Integrate, start up and configure a prepared life system based on Linux as a virtual machine using Oracle VM Virtual Box. The *Tor* browser is part of this image.
- Using the Tor browser, students shall create an interim email accounts for registering with Shodan (using an account, Shodan allows for displaying 50 search results instead of 10 results for non-registered users). Students are tasked to explore the the search engine.
- Next step students shall perform their own searches and gain additional information from the details' pages, Shodan provides about targets. Additionally, search parameters such as *city*, *country*, *geo*, *hostname*, *net* or *os* are integrated in order to narrow down results. More parameters are to be explored by students.
- Finally, the rest based Shodan API (see `https://developer.shodan.io/api` for documentation) is introduced by utilizing the CLI client provided by Shodan itself (`https://cli.shodan.io/`).

Findings

Students observed the very limited efforts, that is required for finding certain devices on the Internet and gaining detailed information about them. Figure 7 shows some statistics about Shodan results in general. Figure 8 shows some details about a search on webcams, which is well-known for vulnerabilities and week credentials. It can be observed, that also export functionality is provided.

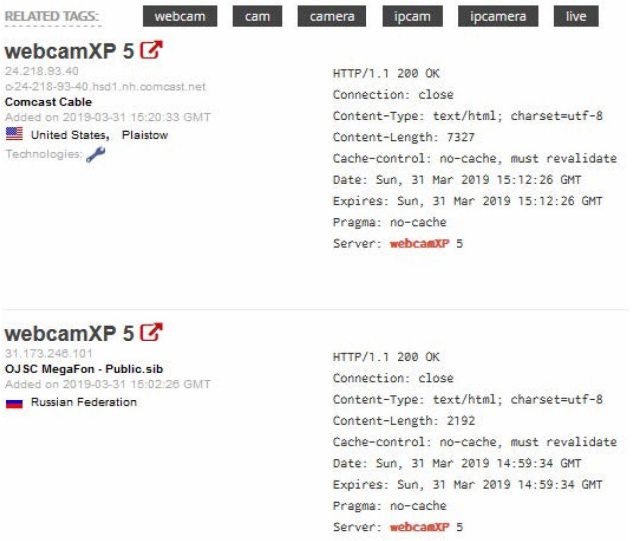


Figure 8. *Screenshot of Shodan website showing details about a search for "webcamxp"*

Details, that are presented on concrete targets, include IP address, host name, ISP, date of entry in the catalogue, country / geographical position. Statistics about searches include the amount targets, the top services (ports), the top operating systems, the top organisations (ISPs) and the top products (names of software).

Search parameters are a massive support for running searches. In addition to the general parameters above, there are also protocol specific parameters available for HTTP, SSL, NTP or Telnet.

Exercise 3: Loxone penetration

This experiment is dedicated to the Loxone Enterprise Smart Home Solution, which was introduced before. Each group of students is assigned a Loxone demo case (see figure 2) for carrying out the exercise.

The following tasks are part of the experiment:

- Starting up the Miniserver of the Loxone demo case and integrating it in the laboratory network infrastructure. Test the user interface of the Miniserver and start controlling the peripheral devices.
- Mini-Introduction to configuring Loxone: Start the programming interface *LoxoneConfig* and download the default program for demo cases from Miniserver. Monitor the behavior using the LiveView feature.
- Adopt minor changes to the program and push it back to Miniserver; activate by rebooting the Miniserver.

Finally students are tasked to carry out basic security analysis starting with a port scan on the Miniserver of the demo case. Find information about the Miniserver regarding open ports, services listening there and the local firewalling of the system.

Findings

As the demo case is coming with a default configuration and program, the Miniserver could be used with its peripheral devices

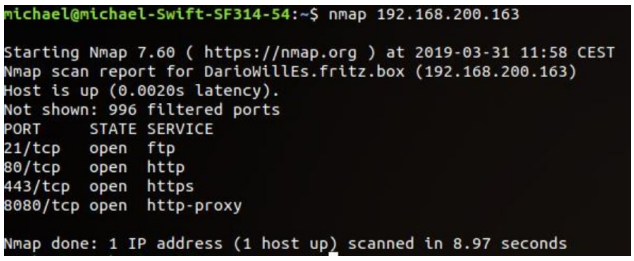


Figure 9. *Result of port scanning Loxone Miniserver using NMAP*

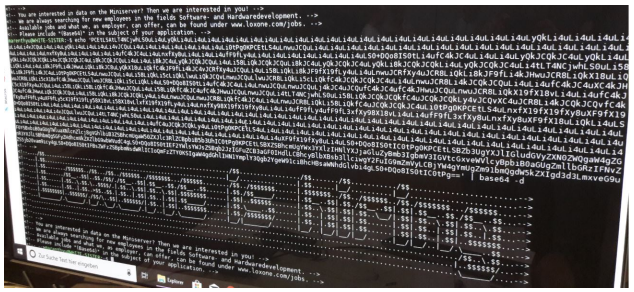


Figure 10. *Base64 decoded credentials file from Loxone image*

straight away.

As shown in figure 9, four TCP ports were found active on the Miniserver. Ports 80 and 443 were dedicated to user interaction including push notifications. On port 21 indeed a FTP server was listening, which did not require authentication (it could be deactivated however).

Via TCP port 21 the students could grab an entire image of the complete file system of the Miniserver. Some further research is possible in order to identify any kind of sensitive information on the file system such as credentials. Indeed, a file *credentials* could be found on the image - however, as shown in figure 10, the manufacturer had deposited this file by purpose.

Exercise 4: Home Assistant with a Raspberry Pi

Home Assistant (`https://www.home-assistant.io`) is a vendor independent open source solution for Smart Homes written in Python. It especially qualifies for deployments on Raspberry Pi computers.

The following tasks are part of the experiment:

- As part of the exercise the students are tasked to install and start-up their own Home Assistant instance on a Raspberry Pi using the specialized distribution *Hassbian*. The deployment are to be integrated in the laboratory network and tested in the first place.
- Next task is on-boarding the deployment by applying an individual configuration and mainly the devices were to be registered. The documentation shall include devices discovered automatically, devices which were registered manually and the challenges when registering Smart Home devices.
- After improving the rule set especially by enhancing the level of automation the lab setup is finally extended by an Alexa device. This is to be integrated with the Home Assistant deployment in order to allow for voice controlling the

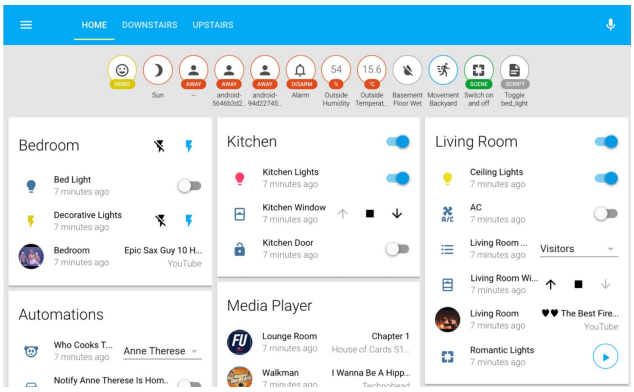


Figure 11. *Sample dash board of Home Assistant (image src: technikblock.de)*

afore defined activities.

Finally, students are tasked to run basic security analysis on the devices as configured before. The students shall carry out a port scan on the Home Assistant as well as the Alexa and document the findings.

Findings

Several devices from within the laboratory could be discovered by the Home Assistant deployment.

The Home Assistant installation causes quite some trouble upon installation and also during usage.

On the Raspberry Pi (running Hassbian) only three TCP ports are open: 22 (SSH), 8123 (Webinterface), dynamic ports $>$ 30000 (XMLRPC). Traffic on the ports other than 22 is HTTP and not HTTPS.

Conclusion

First of all, the course caused major interest among the students. Feedback from the students especially highlighted the hands-on approach on devices and the modern technology used in the experiments.

The trainers experienced major challenges when preparing the sessions, as very limited literature and material is yet available on the topic.

In future instances of the course the trainers are going to:

- increase the initial part on theoretical background on IoT, Smart Home and their security capabilities in order to set a common baseline for among the students for the practical experiments,
- embed the mini projects of the course in wider overall projects in order to enable the students to provide overall progress on analysis of wider security issues in the IoT sphere,
- upgrade the laboratory by additional features; next step will be the integration of software defined radio hardware and software in the lab and its integration in the module.

Keywords

Internet of Things, IoT, Smart Home, Smart Home Security, cybersecurity, connected home.

References

[1] Federal Office for Information Security, Germany: Basisschutz fuer iot smarthome, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/basisschutz_fuer_iot_smarthome.html.

[2] C. Bertko; T. Weber: Home, Smart Home: Der praktische Einstieg in die Hausautomation 2017.

[3] T. F. Collins et al.: Software-Defined Radio for Engineers, Analog Devices, 2018.

[4] P. Hüwe; St. Hüwe: IoT at Home: Smart Gadgets mit Arduino, Raspberry Pi, ESP8266 und Calliope entwickeln. 2019.

[5] O. Shwartz et al.: Reverse Engineering IoT Devices: Effective Techniques and Methods, IEEE Internet of Things Journal, 2018.

[6] F. Völkel: Smart Home - Bausteine für Ihr intelligentes Zuhause. Haufe 2017.

[7] K. Kröger; R. Creutzburg: Conception of a course for professional training and education in the field of computer and mobile forensics, Proc. SPIE 8406, Mobile Multimedia/Image Processing, Security, and Applications 2012, 84060W (8 May 2012), https://doi.org/10.1117/12.923275.

[8] Brandenburg University of Applied Sciences: Studienführer Master 2019/20, https://www.th-brandenburg.de/mediathek/?tx_reintdownloadmanager_reintdlm%5Bdownloaduid%5D=25930&cHash=7b6d3777bef358d91c2d471c5139c68a.

[9] European Commission: European Regional Development Fund (ERDF), https://ec.europa.eu/regional_policy/en/funding/erdf/

[10] I-Intelligence: Open source intelligence tools and ressources handbook 2018, (https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf).

[11] B. van Venrooy: Sicherheit in der Heimautomatisierung, BSc thesis, Hochschule Bonn-Rhein-Sieg, 2016.

[12] EnOcean Alliance: EnOcean Equipment Profiles (EEP), Version 2.6.3.

[13] N. Jurran: Hintereingang inklusive - Fatales Sicherheitsleck beim Smart-Home-System von Loxone (https://www.heise.de/select/ct/2016/19/1473938320762587).

[14] The Guardian: DDoS attack that disrupted internet was largest of its kind in history, experts say (https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet).

[15] Softpedia News: Dyn - DDoS Attack Powered Mainly by Mirai Botnet (https://news.softpedia.com/news/dyn-ddos-attack-powered-mainly-by-mirai-botnet-509541.shtml).

[16] Cisco Talos: Talos Vulnerability Report - TALOS-2019-0888 - EmbedThis GoAhead web server code execution vulnerability, CVE-2019-5096, 02 December 2019 (https://talosintelligence.com/vulnerability_reports/TALOS-2019-0888).

[17] ETSI: TECHNICAL SPECIFICATION (TS) 103 645 - CYBER; Cyber Security for Consumer Internet of Things, Version 1.1.1, Feb. 2019-02 (https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf).

[18] Deutsches Institut für Normung (DIN), Normenausschuss Informationstechnik und Anwendungen (NIA): DIN SPEC 27072 Informationstechnik - IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit (Information Technology - IoT capable devices - Minimum requirements for Information security), May 2019 (https://www.din.de/de/mitwirken/normenausschuesse/nia/din-spec/wdc-beuth:din21:303463577).

Author Biography

Michael Pilgermann has a doctorate in Computer Science with focus on Information Security. He had worked in industry and Federal government, where he gained founded experience in Critical Information Infrastructure Protection. Since 2016 he has been heading the Security Management within the Federal Agency for Public Safety Digital Radio, Germany. Additionally, he has been acting as visiting lecturer at Brandenburg University of Applied Sciences in Brandenburg since 2018.

Since 1992 Thomas Bocklisch has been a Laboratory Engineer in the Department of Informatics and has been responsible for the IoT and Smart Home Security Lab at the Brandenburg University of Applied Sciences in Brandenburg, Germany.

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.

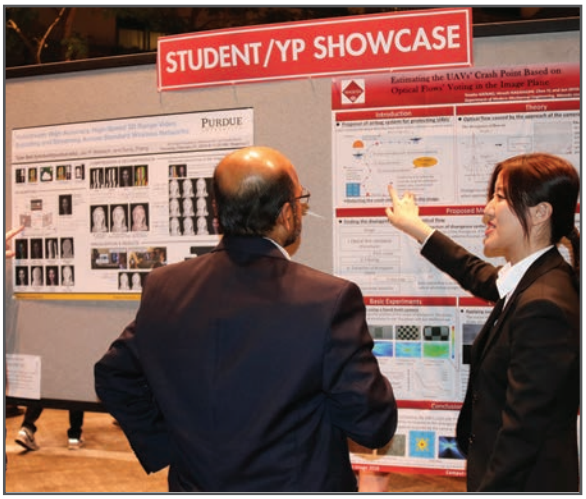
JOIN US AT THE NEXT EI!

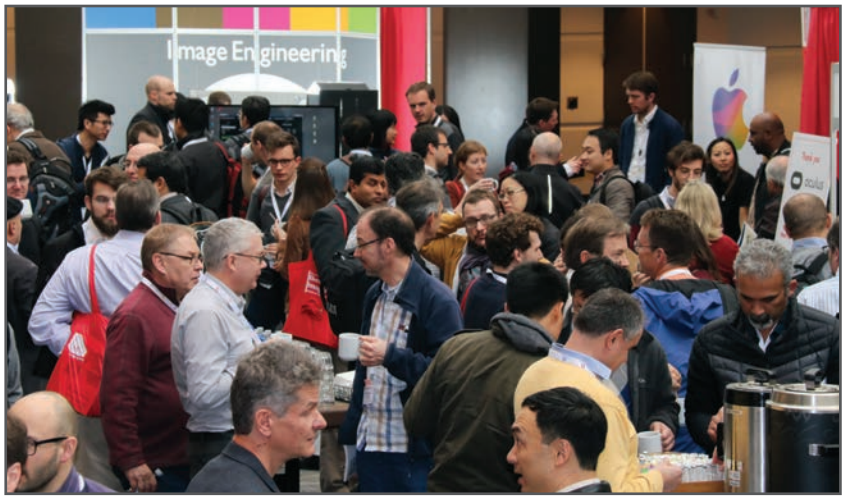
IS&T International Symposium on

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