Cybersecurity by Design for Smart Home Environments

Pragati Siddhanti[1], Petra Maria Asprion[2] and Bettina Schneider[2]
[1]IBM Client Innovation Center Switzerland, Bahnhofstrasse 4, 3073 Gümligen, Switzerland
[2]Competence Center Cyber Security and Resilience, Institute of Information Systems, University of Applied Sciences and Arts Northwestern Switzerland, FHNW, Peter Merian-Str. 86, Basel, Switzerland

Keywords: Cybersecurity by Design, Cyber Risks, Cybersecurity, Internet of Things, Good Practices, Smart Homes.

Abstract: The Internet of Things (IoT) is being increasingly adopted by businesses to improve operations, processes, and products. While it opens endless opportunities, it also presents tremendous challenges especially in the area of cyber risks and related security controls. With billions of interconnected devices worldwide, how do we ensure that they are sufficiently secure and resilient? As a reasonable solution, 'Cybersecurity by Design' seems a promising approach. In this research, 'Smart Homes' - as IoT containing products – are selected as unit of analysis because they are exposed to numerous cyber threats with corresponding adverse consequences for the life, safety and health of residents. By aiming to secure Smart Home Environments (SHEs) from cyber threats, we adopted 'design science' as methodology and developed a holistic approach, highlighting 'good practices', which can be applied in every phase of the SHEs product lifecycle. In addition to these good practices, a 'Cyber Security Maturity Assessment' tool for SHEs has been developed. Both artefacts have already been validated and incrementally improved, and are now awaiting their future application and further enhancements.

1 INTRODUCTION

With billions of people connected to the internet and with the number of connected devices anticipated to exceed 50 billion by the year 2020, the Internet of Things (IoT) represents a major transformative step in the digitized world of today and has the potential to affect everyone and every business (Cisco, 2017; Columbus, 2016).

Per definition, the IoT is a gigantic network of connected 'things', also including people. It refers to the ever-growing network of physical objects identifiable via Internet Protocol (IP) addresses that allow connectivity and communication between these objects and other internet-enabled devices and systems. IoT is an emerging technology, which relies on cloud computing, sensors and thousands of new applications (Evans, 2011; EY, 2015; Minerva et al., 2015). Although IoT products are spreading explosively, security concerns or 'cybersecurity by design' approaches are rarely being discussed so far (Coll and Simpson, 2016).

Given the above outlined complexities in terms of infrastructure, interconnectedness, remote access, it furthers the challenges in areas such as data privacy, data protection, safety, governance and trust (e.g., Elmaghraby and Losavio, 2014; ENISA, 2014a; FTC, 2015a; Grance and Jansen, 2011).

Many studies (e.g., Cisco, 2017; Columbus, 2016) show that 'Smart Homes' as a concept has existed for many years but has gained attention due to the growth of the IoT domain. Smart Homes merge various technologies with the aim to provide a better living experience for their users. These technologies affect areas, which include home appliances, lighting and control systems, entertainment and communication systems in order to allow comfortable activities such as a seamless access to sensors, devices or appliances to communicate with each other or with its users (e.g., Mantas et al., 2010).

SHEs can be defined as devices and systems, associated services as well as the networks used to interconnect all those artefacts, located inside or outside the home environment (Barnard-Wills et al., 2014).

As 'asset groups' can be categorized: software, home networking, audio, visual, storage media, home appliances, sensors, robotics, tags and markers, home security tools, transportation, medical, management/ operation, and people (Barnard-Wills et al., 2014).

Turning back to the challenges, cybercrime has reached an estimated value of up to £34 billion per

Siddhanti, P., Asprion, P. and Schneider, B.
Cybersecurity by Design for Smart Home Environments.
DOI: 10.5220/0007709205870595
In *Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS 2019)*, pages 587-595
ISBN: 978-989-758-372-8

year. Six million people have fallen victim to it in 2016, with 1.4 million reported computer virus attacks, and 650.000 emails and social media profiles stolen (The Telegraph, 2016). Accordingly, while Smart Home Devices (SHDs) are becoming an integral part of our daily lives, security risks pertaining to IoT are showing exponential growth. A study from 2014 (Miessler, 2014) already showed, 70% of IoT devices are vulnerable to an attack. In a world, which relies on internet technology, cyber-attacks are no longer a plot in science fiction novels, but pose immediate challenges at present (ENISA, 2017a). A survey from ENISA revealed that current IoT vulnerabilities are unresolved challenges and that there is a need to incorporate cybersecurity by design towards SHDs (ENISA, 2017b). From this, it can be concluded that the balance between (home) convenience and cyber-security measures is key in the future (Farhoud, 2015).

These findings paved the way for the central theme of this research from two perspectives - from a view of a consumer/user and from a service provider of SHDs. This research aims to support secure Smart Home Environments (SHEs), which should be as much as technically possible resilient against cyber threats throughout its entire life cycle. The latter, we divided into three phases: (1) development, (2) integration, and (3) usage of the SHD.

We directed our investigations with the following question: How can a SHE be secured throughout its lifecycle?

As a main outcome, we designed a prototypical framework with the following four components: (1) collection of potential SHE threats from the cyber space. (2) 'Good practices' in form of checklists and mapped with potential cyber threats. (3) 'Cyber Security Maturity Assessment' tool to evaluate the security of SHDs and related services, and (4) 'Validation' with incremental improvement rounds to evaluate the completeness and usability of the developed artefacts (1-3).

The research follows an inductive approach as the problem understanding as well as the need to secure SHDs/SHEs form the basis of the research and the deployment of artefacts. Furthermore, an inductive procedure offers a flexible structure that allows reacting to changing conditions during research, which is essential due to the dynamics of new technologies. Finally, according to Saunders et al., (2009) investigations inductively designed usually focus on qualitative, rather small data samples, which applies for this research.

The objective of the research - the creation of a framework to secure SHEs throughout its lifecycle - guides towards the design science approach from Hevner and Chatterjee (2010). This approach has been identified as suitable because our research focuses on solving a problem and generating novel artefacts based on rigor and relevance cycles as recommended in the methodology from Hevner and Chatterjee (2010). As main research method, design science was chosen along with qualitative interviews with industry experts in order to collect details from various use cases. Figure 1 shows the foundational research path following the steps suggested by Saunders et al. (2009).

2 CYBERSECURITY

Cybersecurity, refers to the discipline of ensuring that Information and Communication Technology (ICT) systems and devices are protected from attacks and incidents, whether malicious or accidental, threatening the integrity of data, their availability or confidentiality, including attempts to illegally 'exfiltrate' sensitive data or information out of the boundaries of an organization (ITU, 2015).

This applies to network and server environments, as well as to the endpoints (e.g., individual terminals, devices), in-house or mobile. Cybersecurity includes software tools, processes and people as key components of a successful implementation of the discipline (ITU, 2015).

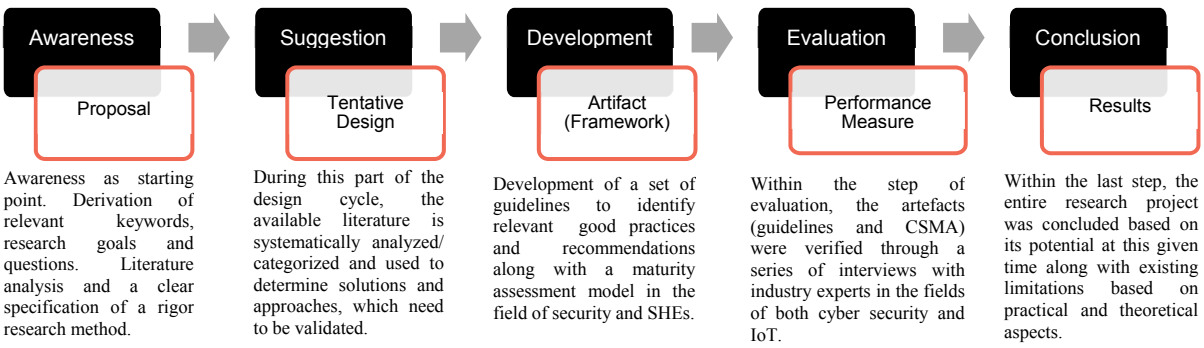

Figure 1: Design science research framework (adapted from Hevner and Chatterjee (2010)).

2.1 Threat Areas

In the following, threat areas are described, which are relevant with regard to SHE cyber threats, vulnerabilities and risks.
By analyzing SHEs, and extrapolating common ICT attacks, threats specific to SHEs can be identified and classified into different threat groups. The potential threats have been adapted from research and practitioner contributions (e.g., Barnard-Wills et al., 2014; Kodra, 2016; O'Brien, 2014; Rehman and Manickam, 2016; Wang and Lu, 2016); they include most of the widely known cyber threats and certain threats, which are specific to SHEs.
These potential threats can be divided into the following areas: (1) physical attacks, (2) accidental damages, (3) loss disasters, (4) outages, (5) failures and malfunctions, (6) eavesdropping, (7) abuse, (8) interception, (9) hijacking, (10) nefarious activities, and (11) control system vulnerabilities.

SHEs are comprised of multiple types of devices and technologies (e.g., protocols, software, hardware, radio communications, operating systems, networks, cloud services). Hence, the known and unknown vulnerabilities in all these areas are relevant (Jacobsson et al., 2016; Barnard-Wills et al., 2014; Draffin, 2016).

The analysis of research and practitioner sources resulted in three different areas of vulnerabilities, which can arise due to (1) business models, (2) design, and (3) the technical devices. Furthermore, the risks associated with SMEs can be categorized as (1) crime risks, (2) data privacy risks and (3) data protection/safety risks.

2.2 Misjudged Risks

An important root cause of insufficient SHDs security are the misjudged risks. For example, the lack of incentives with respect to the device manufacturers, vendors and/or other stakeholders (Elmaghraby and Losavio, 2014; FTC, 2015a, 2015b).

While the IoT industry is growing at an exponential pace, there attention is more focused on the capabilities and the features, which can be delivered. The focus areas are stuck in the 'faster, better and cheaper' strategic segment. Hence, the efforts continue to remain focused in the areas of using more advanced technologies and infrastructures, continuously adding new features and making all of these features available to the consumer at a fast pace while making sure that the cost do not rise (Barnard-Wills et al., 2014; Levy-Bencheton, 2015b). In an equation like this, it is obvious that 'cybersecurity by design' is not of prime priority.

However, cybersecurity by design for SHDs should be prioritized and made part of the strategic agenda for various vendors, device manufacturers and other stakeholders, in order to address the challenges they face in securing their IoT products. This can be regarded as a step in the right direction and has been identified in many forums (e.g., Greverie et al., 2014).

Further risks can be found in underestimating the need for cybersecurity by design, in applying insufficient measures (e.g., FTC, 2015a; ISACA, 2016a; 2016b, 2017; Levy-Bencheton et al., 2015).

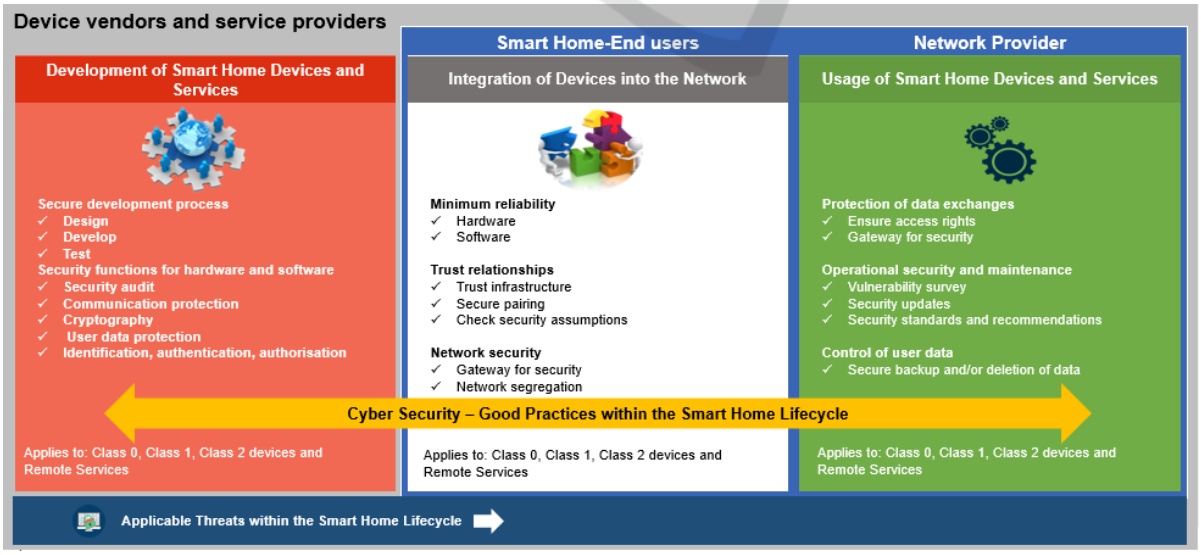

Figure 2: Good Practices for SHEs (adapted from (Levy-Bencheton, 2015b)).

3 GOOD PRACTICES

The primary aim of this research is to create a framework - in the form of a set of good practices (formal guide with recommendations) to mitigate the threats that have been identified in SHEs (see section 2.1). These framework focus on security measures ranging from basic security checklists to dedicated good practices for the entire lifecycle for SHEs.

The set of good practices are organized according to the stakeholders it applies to. We have identified the following stakeholders: (1) 'device vendors', (2) 'service providers', (3) 'network providers' and (4) 'end users'.

The practices are separated into the three phases of the lifecycle of SHDs/SHEs: (1) development, (2) integration and (3) usage. These set of good practices are applicable to the different stakeholders, classes of IoT devices and specific threats. The good practices also separates the recommendations for all these lifecycle related stages to the relevant stakeholder groups: for example, practices which might be applicable to device vendors or service providers as opposed to those, which are valid for network providers or end users.

3.1 Development Phase

During the development phase of a SHD, the SHD manufacturers, vendors and service providers determine the requirements of the product (based on market opportunities and competitor analysis) based on that, they design, develop and test the product.
Safety considerations should also be part of it, triggering measures at the development level of SHDs, including how the various components can be interconnected. These security measures suggest ways, in which the SHEs might be developed by 'design' in order to increase security and reduce impacts upon data privacy. The development phase of the SHD lifecycle consists of two different sets, first 'Secure Development Process', and second, 'Security Functions for Hardware and Software' (Levy-Bencheton, 2015a) as shown in figure 2 (red marked box).

3.1.1 Set for Developers

For developers it is important to have a set of good practices for security by design measures where they can orient themselves for the design of SHDs and related services. This is the pre-condition to set up cybersecurity by design for SHEs. The development process comprises the design, the development and the testing phase (Whitehouse, 2014). For each of these phases, several good practices are derived and integrated in the good practices framework as shown in figure 2 (red marked box).

The most critical aspects being: analyzing threats systematically, defence in depth, isolating security developments from other developments, and making any security related assumptions explicit on the design side. It is during this phase that security functions can be established to ensure security by design based on our set of good practices. In addition, it is also the phase where programming errors may introduce security vulnerabilities (ENISA, 2014a) - for that a procedure is required for finding and remedy such issues. Hence, it is recommended, that stakeholders involved in product, service design and development are forced to work with security-enhancing tools and that training and awareness programs (of potential threats) are mandatory.

Security by design-driven development (Diogenes and Betts, 2017) and implementing the security functions are a key requirement in this phase (Levy-Bencheton, 2015a). For the final part, the testing phase, an emphasis to the compliance of security functions, audits and overall verification of the SHDs and services are some of the highlighted requirements (Coll and Simpson, 2016).

3.1.2 Set for Devices

Security functions address the devices themselves and their interfaces (e.g., web services and mobile apps). The requirements for cybersecurity by design can be categorized as follows (GSMA, 2017b):

- Basic Security Measures – security related events must be logged and users should be notified about every event and uncertainty.
- Networking and Communication – communication should be protected against disclosure, modification, replay and denial of service.
- Cryptography – confidentiality, integrity and authenticity must be protected by using strong cryptography. Keys must be managed securely, and use of a trusted infrastructure is encouraged.
- User Data Protection – confidentiality, inte-grity and authenticity of user data must be protected. Confidentiality protection must be in line with data privacy issues.
- Identification, authentication, authorization – strong authentication methods must be used as well as access control mechanisms. Passwords and sessions should be managed accordingly.
- Self-Protection – hardware and software self-protection should be activated. Data used to

enforce these security functions should be protected and hardening should be used to reduce the attack surface.

All the mentioned security practices should be mandatory and claimed by regulatory bodies – as a foundational good practice or better a mandatory compliance feature which can be audited. An excerpt of the good practices for the development phase is attached in appendix A (figure 4).

3.2 Integration Phase

During the integration phase, the end-user configures and connects its SHD to its Home Area Network (HAN), potentially with the support of the device vendor, the service provider, or the electronic communication provider.

Given the interconnected nature of many SHDs, these practices overlap somewhat with network and communication security measures, and involve measures on the part of the device vendor and associate service providers (TechHome, 2015). Good practices for the device integration can be grouped into three main categories based on network security measures (McKechnie, 2017) and can be ordered in the form of sequence:

1. **Network Security** – It is important to have dedicated security measures for the HAN (e.g., dedicated smart home gateways, service providers set-top boxes, or through service providers (built-in firewalls, antivirus or specialist support).
2. **Security Considerations for Trust** – SHEs should enable trust levels between devices and remote services; for example the establishment of a trust infrastructure within and outside the HAN or secure pairing for SHDs.
3. **Minimum Dependability** – Hardware and software components must provide basic reliability during failures and outages (e.g., user notifications, for network issues switch between available interfaces should be possible or for power failures have battery back-ups in place).

An excerpt of the good practices for the integration phase is attached in appendix B (figure 5).

3.3 Usage Phase

The section above touched on good practices in the SHEs lifecycle focused on the integration phase, which is an important foundation for the overall security approach. In this section, we discuss about the third and final phase of the smart home lifecycle, the usage (and decommission) of SHDs and services. Apart from direct and local interactions with any device, the end-user may also request support from the vendor and use on-line services related to the device through various communication channels. Hence, the usage phase may imply interactions with the device vendor, the service provider, or the electronic communication provider for usage and not least decommission.

The following developed set of good practices have been divided into three parts. The order defined below is based on priority in terms of security importance:

1. **Operational Security and Maintenance** of the SHD - vendors should provide a reliable device update mechanism which allows fixing vulnerabilities on a regular basis. Some of the good practices, which are focused on vendors and users should be carried out periodically, for example to perform vulnerability surveys (Towne, 2014), revisiting security assumptions, security updates and user interface usage and protection (Levy-Bencheton, 2015a).
2. **Secure User Data on the Device** - User data needs to be backed up in a secure manner and stored/processed. Authorized personnel should regularly delete outdated data. In addition, users should be able to delete their private data, which is collected or stored on their SHDs. Moreover, a factory reset and data configuration options should be standard on the device (ENISA, 2017b). Furthermore, data sanitization must be in place for cloud services (Grance and Jansen, 2011).
3. **Protection of Data Exchanges with Networks Accessible to the Device** − the SHD may be interconnected with several networks. In case of an attack on the device or due to a programming error affecting a network, certain separation rules must be followed/established in order to limit the propagation to other networks by techniques such as ensuring access rights and device access management (Levy-Bencheton, 2015a).

An excerpt of the good practices for SHEs in the usage phase is attached in appendix C (figure 6). As a summary, the described phases - development, integration and usage of SHDs - are compiled into the MAS Excel-based checklist of good practices which is mapped to stakeholders (and other dimensions like classes of IoT devices and security threats).

In the following chapter, the developed 'Cyber Security Maturity Assessment' tool - as an

accompanying measure will be introduced. The tool is important for the valuation of the current state of any SHE security status.

4 MATURITY ASSESSMENT

In addition to the development of the framework with good practices for SHEs, a cybersecurity maturity assessment is the second major field of activity within this research. Respectively, this section is going to highlight the essential elements of the maturity assessment along a theoretical baseline adopted from relevant reference models.

4.1 Reference Models

Security reference models are important because they provide an enterprise-wide approach for addressing information security and data privacy requirements within and across systems (The EA Pad, n.d.). For (large) companies/organizations, reference models such as ITIL, COBIT, CMMI, NIST, ISO are well-known and widespread. In the space of IoT and particularly SHEs, there are specific reference models available developed by organizations such as ENISA, OWASP, NIST or ISACA. However, there is no standard maturity measurement model, which is being used to assess the security maturity of IoT devices considering the lifecycle of SHDs or SHEs. A reference model for the maturity assessment should be able to determine the maturity of SHE´s cybersecurity status during the complete lifecycle.

For the purposes of this research, the set of good practices (as outlined in chapter 3) were transferred into related cybersecurity controls to create a tool for the maturity assessment. As theoretical foundation, we combined maturity assessment structures provided from ISACA and NIST. The assessment tool is created according to the stakeholders it applies to; just like the good practices, the assessment is separated into the three phases: development, integration and usage of SHDs and services.

4.2 Maturity Assessment

In order to ignite continuous improvements, security measures need to be classified according to how advanced the device, the environment or service is at a certain time. Thereby various aspects such as system performance or already existing security controls need to be analyzed and rated. Based on such an investigation, each device, environment or service needs to be classified within a model usually containing different levels of maturity.

As visualized in figure 3, the ‘Cyber Security Maturity Assessment’ tool, referred to as CSMA, contains six different levels of maturity, starting from level 0 for ‘not performed’ in case of completely no security controls are placed and moving up to level 5 for ‘comprehensively optimized processes’ (ISO, 2008).

Along these maturity levels, cybersecurity controls, depending upon the type of stakeholders inside the SHE, can be categorized according to their specific strengths and weaknesses. Therefore, the stakeholder governance bodies or IoT providers should launch an initiative of categorizing controls according to their maturity levels. The drafted CSMA contains a comprehensive questionnaire that enables the establishment of the targeted safe SHEs. This CSMA is intended to evaluate the maturity of cybersecurity by design in the context of SHEs considering three dimensions: (1) scope, (2) assessment criteria, and (3) processes. The CSMA aligns the view of STOPE (Strategy, Technology, Organization, People, and Environment) for scoping (Saleha and Alfantookh, 2011); while its assessment criteria are considered to be open to various standards. As an example, an excerpt of the CSMA, which has been created using MS Excel, including macros and advanced functions.

5 VALIDATION

After finishing the development of a prototypical good practices and CSMA, we started a selection of industry experts in the area of IoT and (cyber) security (by design) and expertise for SHDs/SHEs. Therewith, a group of five professional experts with different roles and complementary industry background were carefully handpicked. The framework of good practices and the CSMA was presented for evaluation and feedback. Once the framework was circulated, the experts validated the goal, usability and capability of the framework and the CSMA in practical scenarios. During this process, various improvement potentials were identified and adaptions were made and tested in iterative cycles.

Overall, the qualitative feedback from the five professional experts has highlighted the potential of the framework with the good practices and the associated CSMA. Both are recognized as valuable and applicable instruments for SHD manufactures, vendors, solution and service providers along with network providers.

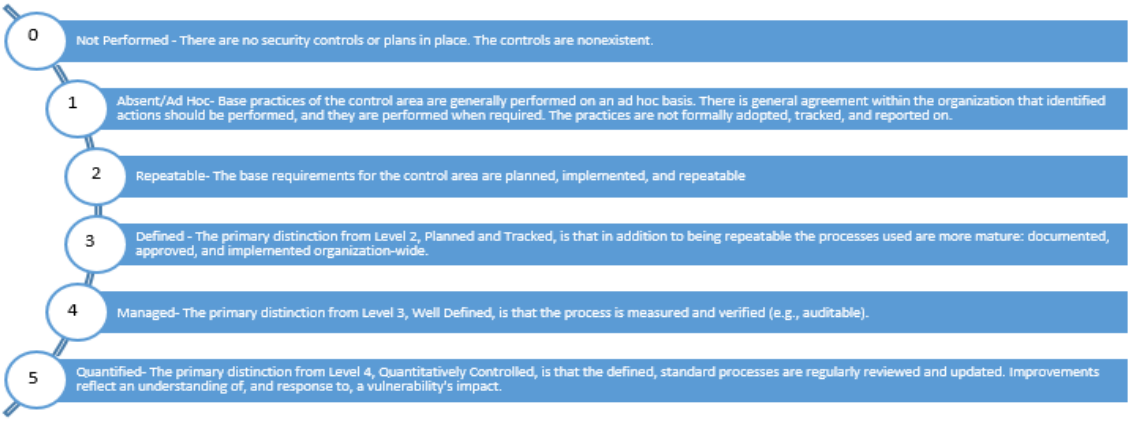

Figure 3: CSMA Maturity Levels (adapted from ISO 21827:2008 (ISO, 2008)).

6 CONCLUSION AND OUTLOOK

This research has been conducted to explicate the risks, which exist in the context of SHEs and how they can be mitigated. The results are an attempt to bridge the identified gap with regard to 'cybersecurity by design' and functionality of SHDs/SHEs and related services. The first result, the set of good practices allows stakeholders to build - as precondition - secure SHDs and services 'by design'. The second result, the CSMA for SHEs helps to evaluate and measure the cybersecurity status of existing SHDs/SHEs.

Based on the results of the design science guided research with a strong focus on the development and validation of applicable artefacts several prospective research fields for further improvement of the good practices (chapter 3) and the CSMA (chapter 4) are identified.

First, with regard to the CSMA, an assessment of all dimensions of SHEs is currently not possible with the prototypical version of the tool, as the research needed defined limits from the onset. However, the prototypical CSMA is developed so far that it could be used as a valuable foundation for SHD software development companies to assess the maturity of SHDs or SHEs and to get an 'idea' about their current status or gross control gaps. Nevertheless, further research activities should be performed to identify opportunities to extend the developed artefacts with additional dimensions.

Another worthy field of prospective research is to define the optimized state or the minimal maturity score of a particular SHD. This could be used as an industry practice for the development of a quality seal for SHDs with 'cybersecurity by design' components. While the need for cybersecurity by design measures has been identified, the minimum security requirement before SHD product release are a potential further evolution step.

As another potential and important field of activity, further optimization of the good practices set and its techniques is recommended. In its current state, the good practices are defined within an MS Excel sheet, what allows on the one hand automated calculations of various elements. On the other hand, the composed formulas are closely associated with the research work and they need probably to be more holistic for a professional or large-scale application.

Finally, a professionalization of the prototype and more extensive validation is required to improve the presented artefacts. After that, the result could be extremely valuable for the practice and be used rather quickly.

REFERENCES

Barnard-Wills, D., Marinos, L. & Portesi, S., 2014. Threat Landscape and Good Practice Guide for Smart Home and Converged Media. EU.

Cisco Systems, 2017. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021. White Paper. Retrieved from http://tinyurl.com/zzo6766.

Columbus, L., 2016. Roundup of Internet of Things Forecasts and Market Estimates. Forbes. Retrieved from http://tinyurl.com/yar5llet.

Coll, L. & Simpson, R., 2016. The Internet of Things and challenges for consumer protection. London, UK.

Diogenes, Y. & Betts, D., 2017. Internet of Things security best practices. Retrieved from www.docs.microsoft.com.

Draffin Jr, C. W., 2016. Cybersecurity White Paper. MIT Energy Initiative utility of the future. Retrieved from https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf.

Elmaghraby, A. S. & Losavio, M. M., 2014. Cyber security challenges in Smart Cities: Safety, security and privacy.

Journal of Advanced Research, 491-497.
ENISA, 2014a. Privacy and Data Protection by Design – From policy to engineering. Retrieved from www.enisa.europa.eu.
ENISA, 2017a. Principles and opportunities for a renewed EU cyber security strategy. Retrieved from www.enisa.europa.eu.
ENISA, 2017b. Cloud Computing Certification - CCSL and CCSM. Retrieved from www.enisa.europa.eu.
Evans, D., 2011. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. San Jose, CA, USA.
EY, (2015). Cybersecurity and the Internet of Things. US. EYGM Limited. Retrieved from www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf.
Farhoud, N., 2015, How hackers could use your 'smart home' devices to break into your home and spy on your kids. Retrieved from http://www.mirror.co.uk/tech/smart-home devices-could-criminals-10361249.
FTC, 2015a. Privacy & Security in a Connected World. Retrieved from www.ftc.gov/system/files/documents/report/federal-trade-commission-staff-report-november 2013-workshop-entitled-internet-things privacy/150127iotrpt.pdf.
FTC, 2015b. Careful Connections: Building Security in the Internet of Things. Retrieved from www.ftc.gov.
Grance, T. & Jansen, W., 2011. Guidelines on Security and Privacy in Public Cloud Computing. Retrieved from www.nist.gov.
Greverie, F., Buvat, J., Nambiar, R., Appell, D. & Bisht, A., 2014. Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT. Capgemini Consulting.
GSMA, 2017a. IoT Connection Efficiency Guidelines. Retrieved from www.gsma.com/iot/gsma-iot-device connection-efficiency-guidelines/.
GSMA, 2017b. Remote Provisioning Architecture for Embedded UICC Test Specification. Retrieved from www.gsma.com/newsroom/wp-content/uploads//SGP.11-v3.3.pdf.
Hevner, A. R. & Chatterjee, S., 2010. Design Research in Information Systems. New York (USA), 1. ed., Springer Science and Business Media LLC.
ISACA, 2016a. IoT Needs Better Security. ISACA Journal, vol. 3, 27-32.
ISACA, 2016b. Security Assurance in the SDLC for the Internet of Things. ISACA Journal, vol. 3, 32-43.
ISACA, 2017. Managing the Risk of IoT. ISACA Journal, vol 3, 19-27.
ISO, 2008. Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model (SSE-CMM). Retrieved from www.iso.org /standard/44716.html.
ITU, 2015. Cybersecurity, data protection and cyber resilience in smart sustainable cities. International Telecommunication Union. Focus Group Technical Report. Retrieved from www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc.
Jacobsson, A., Boldt, M. & Carlsson, B., 2016. A risk analysis of a smart home automation system. Future Generation Computer Systems, 719-733.
Kodra, S, 2016. Smart Home Hacking, NTNU. Retrieved from https://brage.bibsys.no/xmlui/bitstream/handle/11250/2405119/15721_FULLTEXT.pdf?sequence=1.
Levy-Bencheton, C., 2015a. Security and Resilience of Smart Home Environments. Retrieved from www.enisa.europa.eu.
Levy-Bencheton, C., 2015b. Securing the Lifecycle of Smart Home Environments. Retrieved from www.enisa. europa.eu.
Levy-Bencheton, C., Darra, E., Tetu, G., Dufay, G. & Alattar, M., 2015. Security and Resilience of Smart Home Environments. Retrieved from www.enisa.europa.eu.
Mantas, G., Lymberopoulos, D. & Komninos, N., 2010. Security in smart home environment, Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications. Medical Information Science, Hershey, 170-191.
McKechnie, G., 2017. Integrating Smart Home Devices. Retrieved from http://smarthomegallery.com/insights/integrating smart-home-devices/.
Miessler, D., 2014. HP Study. Retrieved from community.saas.hpe.com/t5/Protect-Your Assets/HP-Study-Reveals-70-Percent-of-Internet of-Things-Devices/ba-p/220516#.WT7x6BOGPR2.
Minerva, R., Biru, A. & Rotondi, D., 2015. Towards a definition of the Internet of Things (IoT).
O'Brien, D., 2014. The Internet of Things: New Threats Emerge in a Connected World. Retrieved from www.symantec.com/connect/blogs/internetthings-new-threats-emerge-connected-world.
Rehman, S. U. & Manickam, S., 2016. A Study of Smart Home Environment and its Security Threats. In International Journal of Reliability, Quality and Safety Engineering.
Saleha, M. S. & Alfantookh, A., 2011. Applied Computing and Informatics. A new comprehensive framework for enterprise information security risk management, 107-118.
Saunders, M. N., Lewis, P. & Thornhill, A., 2009. Research Methods for Business Students. 5. ed. Harlow, England, Pearson Education Limited.
TechHome, 2015. Recommended Best Practices for Securing Home Systems. Retrieved from www.cta.tech/cta/media/Membership/PDFs.
The EA Pad, n.d.. Reference Models. Security Reference Model – SRM. Retrieved from eapad.dk/gov/us/common-approach/reference-models/.
The Telegraph, (2016). Cyber-crime: One in 10 people now victim of fraud or online offences, figures show. Retrieved from www.telegraph.co.uk/news/2016/07/21/one-in-people-now-victims-of-cyber-crime/.
Towne, S., 2014. The Current State of Smart Locks. Retrieved from http://schuylertowne.com/blog/smart-locks.
Wang, W. & Lu, Z., 2013. Cyber security in the Smart Grid: Survey and challenges. In Computer Networks, 1344–1371.
Whitehouse, O. (2014). Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond. Retrieved from www.nccgroup.trust.

APPENDIX A

The Develoment Of Smart Home Devices & Services		Classes of Smart Home Devices				
f the development process		APPLIES TO				
Design phase		Class 0 devices	Class 1 devices	Class 2 devices	High capacity devices	Remote services
	Use defence in depth – multiple layers of security controls (defence) are placed throughout an information technology (IT) system		✓	✓	✓	✓
	Isolating security developments from other developments		✓	✓	✓	✓
	Make assumptions for the security requirements explicit		✓	✓	✓	✓
	Consider third-party review by security specialists rather than developers with limited security experience		✓	✓	✓	✓
	Analysing threats systematically		✓	✓	✓	✓
	Prepare user interactions with the devices or services	✓	✓	✓	✓	✓
Development phase						
	Use configuration management tools, and leverage upon development environments such as compilers or static analysers		✓	✓	✓	✓
	Take security into account when choosing your programming language; when available, leverage upon the operating system se		✓	✓	✓	✓
	Use standard, secure frameworks or stacks whenever possible – do not redevelop security functions		✓	✓	✓	✓
	Ensure team training and awareness		✓	✓	✓	✓
Testing phase						
	Test the compliance of security functions		✓	✓	✓	✓
	Perform additional security audits and penetration testing		✓	✓	✓	✓
	Perform a privacy assessment		✓	✓	✓	✓
unctions for hardware and software						
Security audit						
	Log security events		✓	✓	✓	✓
	Notifications should be easy to understand and help users find a remediation or workaround		✓	✓	✓	✓

Figure 4: Excerpt of the Good Practices for SHEs (Development Phase).

APPENDIX B

Best Practises For The Integration Of Smart Home Devices & Services into the Network			Classes of Smart Home Devices				
			APPLIES TO				
		Minimum Reliability	Class 0 devices	Class 1 devices	Class 2 devices	High capacity devices	Remote services
		Hardware must provide basic reliability measures to resist outages and jamming	✓	✓	✓	✓	
		Software components of the Smart Home must handle data changes without failure, errors and improper functioning	✓	✓	✓	✓	
		Trust Relationships					
		Use a trust infrastructure within and outside the HAN		✓	✓	✓	✓
		Use secure pairing for devices		✓	✓	✓	✓
		Check the security assumptions at installation time		✓	✓	✓	✓
		Network Security					
		Introduce a gateway to mitigate the propagation of attacks from or to the HAN		✓	✓	✓	✓
		Network segregation as additional security measure		✓	✓	✓	✓

Figure 5: Excerpt of the Good Practices for SHEs (Integration Phase).

APPENDIX C

Best Practises For The Usage untill End- of-Life Of Smart Home Devices & Services				Classes of Smart Home Devices				
	Protection of Data Exchanges			APPLIES TO				
				Class 0 devices	Class 1 devices	Class 2 devices	High capacity devices	Remote services
			Ensure access rights	✓	✓	✓	✓	✓
			Leverage on gateways to reduce the network exposure of the weaker devices	✓	✓	✓	✓	
			Segregate the Smart Home Networks and the AMI	✓	✓	✓	✓	
	Operational Security and Maintainence							
		Vulnerability survey						
			Perform vulnerability survey	✓	✓	✓	✓	✓
			Revisit security assumptions on a regular basis	✓	✓	✓	✓	✓
		Security updates						
			Protect the software update mechanism		✓	✓	✓	
		Remote interfaces protection						
			Provide user-friendly interfaces for device and services security management		✓	✓	✓	✓
			Protect remote monitoring interfaces		✓	✓	✓	✓
		Security management system for support infrastructures						
			Rely on existing sources for security good practices in order to secure infrastructures		✓	✓	✓	✓
	Control of User Data							
			Provide secure backup and/or deletion of the data stored/processed by the device (and by associated cloud services) during the operation and at end-of-life		✓	✓	✓	✓

Figure 6: Excerpt of the Good Practices for SHEs (Usage Phase).