Design and Justification of a Cybersecurity Assessment Framework for IoT-Based Environments

Luit Verschuur(✉)

LIACS, Leiden University, Leiden, The Netherlands
Luit_ver@live.nl

Abstract. Today, our world is more connected than ever. One of the main drivers of this connection is the uprise of the Internet of Things (IoT). Associated with this rise, there are numerous challenges. One of the main challenges for IoT is to keep the environments that include IoT devices secure. IoT devices are different from traditional computer devices. Therefore, they need special treatment and guidance to be kept secure. This research identifies the limitations of current assessment frameworks to cover IoT-specific challenges. It discusses the possible assessment methods to assess these challenges. In addition, the potential solutions to secure these environments are listed. Afterward, the processes and guidelines that can be implemented are identified. All to generalize these findings into an overall applicable cybersecurity assessment framework for IoT-based environments. These steps are validated by existing research, existing cybersecurity frameworks, and interviews with cybersecurity experts. Together, these sources provide valid ground to guide IoT-based environments to improve security with the assistance of an assessment framework. This IoT assessment framework is the first of its kind and therefore valuable for all IoT-based environments. However, it still needs to improve to reach its full potential.

Keywords: Internet of Things (IoT) · IoT-based environments · IoT specific challenges · security and protection · assessment methods · cybersecurity assessment framework

1 Motivation

Today, our world is more connected than ever. This connection is continuously spurred by technological advancements. One of the main advancements in recent years was the upcoming of the Internet of Things (IoT). IoT has been called the trend of the next internet by Gokhale et al. (2018), due to the expected large role it will play in our lives. IoT is defined as a global cyber-physical network of interconnected embedded objects. Besides the positive possibilities of IoT, there are also downsides to this trend. The implementation of IoT comes with major challenges and concerns. The major challenge that Alkhalil and Ramadan (2017) identified, is that IoT encounters high security risks.

B. Hämmerli et al. (Eds.): CRITIS 2022, LNCS 13723, pp. 49–55, 2023.
https://doi.org/10.1007/978-3-031-35190-7_4

In more detail, there are millions of IoT devices in use that do not meet the existing security standards. Therefore, there is a need to properly secure IoT-based environments. As IoT has specific characteristics, it has to deal with other types of challenges than traditional computing devices. This implies that the current assessment frameworks do not apply to IoT-based environments. Therefore, the research objective is to develop an IoT-specific assessment framework to secure IoT-based environments. This is relevant as there is no existing assessment framework focusing purely on the security of IoT-based environments. The main research question that will provide this framework is:

How to assess challenges and differences in the security of IoT-based environments, compared to the security of traditional computing devices?

The main research question treated in this article is divided into 5 subquestions. These are the following:

- **SQ1:** *What are the limitations of the available cybersecurity assessment frameworks for IoT-based environments?*
- **SQ2:** *How can risks in IoT-based environments be assessed?*
- **SQ3:** *What are potential solutions to minimize the risks in IoT-based environments?*
- **SQ4:** *What overall process or guidelines can be implemented to improve the security of IoT-based environments?*
- **SQ5:** *How can the IoT-based environment security be generalized into an overall applicable assessment framework?*

Together, the answers to these questions will provide the assessment framework with a substantial theoretical base. The answers to the first three subquestions are based on previous research. This contribution summarizes the main results, present the framework, and at the end proposed a contribution of that innovative used path.

2 Cybersecurity Assessment Frameworks Limitations IoT

Currently, cybersecurity assessment frameworks fail on two different levels. The first level is the framework itself. On this level, Dardick (2010) states that frameworks often fail to be comprehensive in what components are included and assessed. In addition, Leszczyna (2021) issues that a lot of frameworks fail to be applicable. The second level focuses on the IoT-specific challenges that are neglected. Karie et al. (2021) identified five major challenges for current IoT security frameworks. These five challenges are: technical-, legal-, ethical-, operational-, and adaptive. These challenges need to be covered by a new IoT cybersecurity assessment framework. This is the motivation of the contribution that will be developed in the next paragraph.

2.1 Assessing the Risks in IoT

The limitations that are identified in the previous section, need to be assessed in detail. On the framework level, comprehensiveness can be measured by the extensiveness of the framework. This can be validated by covering all important components. In addition, Eldh et al. (2006) created a method to test the applicability of a framework. On the IoT challenges level, the assessment of these challenges is similar to the assessment of traditional computing devices. However, the challenges that need to be accounted for are different. These challenges need to be identified. Afterward, these can be assessed in the same way as the current best practice. Currently, the best known and most used cybersecurity assessment framework is from NIST created by Barrett et al. (2018). In the following paragraph we refer to IoT-specific challenges.

2.2 Proposed Solutions to Minimize the Risks in IoT

The IoT-specific challenges also need to be solved. In research, two levels of security solutions are proposed. The first level is environment-based, Patel et al. (2016) designed a secure implementation of the architecture of IoT-based environments. The second level is device-based, which means that solutions secure the design of IoT devices. These solutions differ for every device and solve specific security challenges. In addition, cybersecurity will always be based as good as the best and latest developments.

Four key research areas that keep improving the security level in environments are encryption, authentication, blockchain, and intrusion detection systems. Furthermore, all additional implemented solutions provide an extra security layer. Therefore, it is desirable to implement a variety of solutions concerning different challenges. The framework should include these different solutions that are summarized in the following section.

3 Framework Integration: Research by Design

The approach has the objective to propose a new concepted assessment framework; Therefore, the necessary method was *research by design*. This implies that all the design choices are validated. As the assessment framework is the first of its kind, an *explorative research design* is chosen to keep possible implementations broad. In addition, the availability of cybersecurity and IoT experts is limited. Therefore, a *qualitative research method* is chosen to retrieve the full potential of the information gained from every expert. The method that is chosen to retrieve the information from the experts is *interviews*.

These interviews were all conducted with PwC employees. In this approach, 10 different experts are interviewed, who vary in expertise, role, experience, education, and country. Due to the variation in the country, the choice was made to conduct the interviews in a digital environment.

The data retrieved from the interviews are analyzed with the *grounded theory*. This interview analysis method is most excepted because it provides the most

guidance to validly interpret the findings. The eight steps of this method are identified by Online (2009).

1. Identify the substantive area, area of interest
2. Collect data about the substantive area
3. Open code the data when it is collected
4. Write memos throughout the entire process
5. Conduct selective coding and theoretical sampling
6. Sort the memos and find the codes that can organize the codes the best
7. Read the literature and integrate the theory with the codes
8. Write up the theory

Within this method, there is chosen for *open coding* by the researcher as there was no independent researcher available. In addition, to maximize the relevance of the retrieved data, *intermediate labeling* is applied.

4 Framework Design

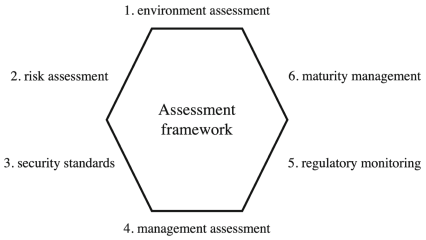
To design the framework based on the different results and discuss these results, the eight steps of the grounded theory are followed: The first step is discussed in the literature review section. The second, third (*open coding*), and fourth (*intermediate labeling*) step are discussed in the methodology section. Together, these four steps have conducted 550 codes. In step five these codes are cleaned, similar codes are combined and double codes are eliminated. This step decreased the number of codes to 238. Afterward, step six sorted these memos to the subquestion they were relevant to, and organized them into categories and subcategories. After this step, every subquestion got a list of relevant categories, subcategories, and concepts to discuss and integrate with the earlier retrieved theory. In the following subsections, the most remarkable results are discussed:

The currently most relevant assessment frameworks are NIST by Barrett et al. (2018), CIA by Fenrich (2008), and IEC by IEC (2022). In addition, the most relevant work in IoT security is done by ENISA by Gines et al. (2017), IoTSF by WG1 (2021), and IEC 62443 by IEC (2020). Together, the scope included in this research is the scope that these frameworks cover collectively. Furthermore, the five main challenges by Karie et al. (2021) are highlighted.

The importance of comprehensiveness, the five main challenges, and the applicability are verified. The comprehensiveness and applicability should be considered in the evaluation of the assessment framework.

The five main challenges (technical, legal, ethical, operational, and adaptive) should be included in the assessment framework to generate structure. All categories can be assessed by six elements:

1. environment assessment
2. risk assessment
3. security standards
4. management assessment
5. regulatory monitoring
6. maturity management



The range of solutions to improve the security of IoT-based environments is very broad. Most solutions that are retrieved from the literature and frameworks are verified by the interviewees. In addition, the solutions retrieved from the interviews are backed by research. Therefore, all the identified solutions could be included in the assessment framework.

The NIST cybersecurity framework by Barrett et al. (2018) will be used as the standard baseline. This baseline is complemented with the most important IoT solutions. These solutions can be found in the work of ENISA, IoTSF, and IEC 62443. In addition, solutions from research and retrieved data will be included to maximize the information in the assessment framework. In this framework, the six elements must be included.

The generated framework was able to include most of the desired characteristics of a new IoT assessment framework. However, the framework could not yet test the applicability of the assessment framework. In addition, the final assessment framework is not yet validated by experts. Furthermore, the regulatory challenge could not be solved. This framework does guide regulators to focus. However, is not able to solve the challenges. These limitations imply that the final assessment framework is not flawless yet. However, it does provide a lot of guidance for best practices in IoT-based environments. In addition, IoT security and its frameworks must be updated, as it is still a fast-changing field.

5 Optimization of the Framework

In this contribution, the theory is the final step of the optimization process of the assessment framework. The framework is based on the IoT challenges in NIST. In Fig. 1, the IoT challenges for the NIST framework categories are illustrated. In the core framework, also the solutions and best practices are provided to solve these challenges.

FUNCTION	CATEGORY	CHALLENGES
ID. IDENTIFY	AM. Asset Management	Technical, legal, ethical, operational, and adaptive
	BE. Business Environment	Technical and operational
	GV. Governance	Technical, legal, ethical, operational, and adaptive
	RA. Risk Assessment	Technical, legal, ethical, operational, and adaptive
	RM. Risk Management Strategy	Technical, legal, ethical, operational, and adaptive
	SC. Supply Chain Risk Management	Technical, legal, ethical, operational, and adaptive
PR. PREDICT	AC. Identity Management and Access Control	Technical, legal, ethical, operational, and adaptive
	AT. Awareness and Training	Technical, legal, ethical, operational, and adaptive
	DS. Data Security	Technical, legal, ethical, operational, and adaptive
	IP. Information Protection Processes and Procedures	Technical, legal, ethical, operational, and adaptive
	MA. Maintenance	Technical, legal, ethical, operational, and adaptive
	PT. Protective Technology	Technical, legal, ethical, and operational
DT. DETECT	AE. Anomalies and Events	Technical, operational, and adaptive
	CM. Security Continuous Monitoring	Technical, legal, ethical, and operational
	DP. Detection Processes	Technical
RS. RESPOND	RP. Response Planning	Technical, operational, and adaptive
	CO. Communications	Technical, operational, and adaptive
	AN. Analysis	Technical
	MI. Mitigation	Technical, operational, and adaptive
	IM. Improvements	Technical, operational, and adaptive
RC. RECOVER	RP. Recovery Planning	Technical
	IM. Improvements	Technical
	CO. Communications	Technical and legal

Fig. 1. IoT challenges related to the NIST categories

These solutions and best practices are based on literature. This literature can either have a challenge specific or have a more global focus.

6 Outlook

The generated assessment framework has a lot of advantages but also still faces limitations. However, the assessment framework is certainly adding value to the academic field of IoT security. Currently, the most important cybersecurity assessment frameworks fail to identify the five main IoT challenges (technical, legal, ethical, operational, and adaptive) by Karie et al. (2021).

In addition, the security standards have little focus on IoT-specific devices. The research and frameworks that do focus on IoT specifically are often only proposing single good practices but are not translated to assessment frameworks. This research translates good practices into an assessment framework for IoT-based environments and translates an IoT-specific assessment framework towards an IT, OT, and IoT converged cybersecurity assessment framework that can be applied to all environments that include embedded devices. Therefore, this contribution leads to new insights towards safer IoT-based environments.

Acknowledgements. The author acknowledges the generous support from the research internship agency PwC. In addition, the guidance offered by Nele Mentens and Stefan Pickl have made this research a success.

References

Alkhalil, A., Ramadan, R.A.: Io T data provenance implementation challenges. Procedia Comput. Sci. **109**, 1134–1139 (2017). 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16–19 May 2017, Madeira, Portugal

Barrett, M.P., et al.: Framework for improving critical infrastructure cybersecurity version 1.1 (2018)

Dardick, G.S.: Cyber forensics assurance (2010)

Eldh, S., Hansson, H., Punnekkat, S., Pettersson, A., Sundmark, D.: A framework for comparing efficiency, effectiveness and applicability of software testing techniques. In: Testing: Academic and Industrial Conference-Practice And Research Techniques (TAIC PART'06), pp. 159–170. IEEE (2006)

Fenrich, K.: Securing your control system: the "CIA triad" is a widely used benchmark for evaluating information system security effectiveness. Power Eng. (Barrington, Ill.) **112**(2), 44 (2008)

Gines, A., Lorente, F., Perez, J., de la Torre, A., Babón, O.: Baseline security recommendations for Io T, November 2017

Gokhale, P., Bhat, O., Bhat, S.: Introduction to Io T. Int. Adv. Res. J. Sci. Eng. Technol. **5**(1), 41–44 (2018)

IEC: Quick start guide: an overview of ISA/IEC 62443 standards, ISA global cybersecurity alliance, June 2020

IEC: Information security, cybersecurity and privacy protection. Standard, International Organization for Standardization, Geneva, CH, February 2022

Karie, N.M., Sahri, N.M., Yang, W., Valli, C., Kebande, V.R.: A review of security standards and frameworks for Io T-based smart environments. IEEE Access **9**, 121975–121995 (2021)

Leszczyna, R.: Review of cybersecurity assessment methods: applicability perspective. Comput. Secur. **108**, 102376 (2021)

Online, G.T.: What is grounded theory? (2009). https://www.groundedtheoryonline.com/what-is-grounded-theory/. Accessed 16 Mar 2022

Patel, K.K., Patel, S.M., et al.: Internet of things Io T: definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. **6**(5) (2016)

WG1, I.S.: Io TSF Io T security assurance framework release 3.0 Nov 2021, November 2021