POSTER: IoT System Trustworthiness Assurance

Razvan Beuran
Sian En Ooi
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan

Abbie O. Barbir
CVS Health
Hartford, Connecticut, USA

Yasuo Tan
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan

ABSTRACT

As the Internet of Things (IoT) becomes more and more pervasive, encompassing many aspects of our daily life, the issue of how much the IoT systems can be trusted is critical. However, the multitude of recent incidents that were caused by or somehow involved such systems, often with dire consequences, makes it obvious that IoT system trustworthiness is not yet attained.

In this paper we provide an overview on IoT trustworthiness, and introduce a trustworthiness assurance methodology based on the novel concept of Trustworthiness Assurance Levels (TALs). The methodology is intended for analyzing IoT systems to determine the degree of confidence one can have that they will perform as expected for a given deployment, taking into consideration external disturbances, system errors, faults and attacks. The paper also includes a case study discussion to demonstrate the applicability of the proposed methodology.

CCS CONCEPTS

• **Computer systems organization** → **Dependable and fault-tolerant systems and networks**; *Embedded and cyber-physical systems*; • **Security and privacy** → Formal methods and theory of security.

KEYWORDS

Internet of Things (IoT), Cyber Physical Systems (CPS), trustworthiness assurance, System of Systems (SoS)

ACM Reference Format:
Razvan Beuran, Sian En Ooi, Abbie O. Barbir, and Yasuo Tan. 2022. POSTER: IoT System Trustworthiness Assurance. In *Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (ASIA CCS '22), May 30–June 3, 2022, Nagasaki, Japan.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3488932.3527287

1 INTRODUCTION

In response to the growing threats regarding Internet of Things (IoT) systems, efforts have been undertaken by various governments and organizations to define guidelines and requirements pertaining to this issue, especially for the security aspects of IoT devices. A representative example on the government side are the secure IoT development guidelines that have been released by the European Union Agency for Cybersecurity (ENISA) [3], and on the organization side the IoT security guidelines and assessment methodology published by the GSM Association (GSMA) [7]. However, these documents do not consider the trustworthiness of IoT systems from other points of view, such as safety, reliability, etc.

To the best of our knowledge, the issue of IoT trustworthiness has only been addressed by few organizations, such as the work done by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) committee "Internet of things and digital twin" JTC 1/SC 41 [11], the Industrial Internet Consortium (IIC) [8], and the U.S. National Institute of Standards and Technology (NIST) Cybersecurity for IoT Program [17].

A more comprehensive look on *trustworthiness assurance* is nevertheless needed, and our research endeavors to enhance the current state in this field by defining assurance levels for trustworthiness. This makes it possible to characterize the degree of confidence one can have that an IoT system will function as intended, depending on the type of methods used to assess its trustworthiness. The core contributions of this paper are as follows:

- Provide an overview of the main aspects concerning the trustworthiness of IoT systems, and its practical assessment
- Introduce a methodology based on assurance levels for verifying the trustworthiness of IoT systems, and illustrate its application in the real world via a case study

2 IOT TRUSTWORTHINESS OVERVIEW

Trustworthiness of CPS, and by extension IoT, is discussed by NIST in its CPS framework [6], but the concept is not explicitly defined, and it is only indicated that trustworthiness includes security, privacy, safety, reliability, and resilience. The issue is very timely though, as evidenced by the 2021 ISO/IEC standard on integrating IoT trustworthiness into system engineering processes [10], and the recent NIST white paper draft regarding the mechanisms needed to establish confidence in IoT device security [15].

A more comprehensive analysis of IoT trustworthiness, in particular in the context of Industrial IoT (IIoT), has been done by IIC, who has proposed a definition that we consider the best available at present, as follows [1]:

> **Trustworthiness** Degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks.

In the next paragraphs we discuss aspects pertaining to the practical assessment of each trustworthiness component.

Safety. Safety issues are commonly dealt with via standards, laws and regulations that manufacturers need to comply with. Hence,

ASIA CCS '22, May 30–June 3, 2022, Nagasaki, Japan.

ACM ISBN 978-1-4503-9140-5/22/05.
https://doi.org/10.1145/3488932.3527287

verifying that the safety requirements of a system are met typically means checking that those standards, laws and regulations have been taken into account during design, and that there are no infringements during system operation. Such regulations are specific to given industries, and may even differ depending on the country. Considering the example of the automotive industry, ISO published a standard on road vehicle functional safety [9], and the Japan Automobile Manufacturers Association (JAMA) published a framework on self-driving safety assessment [13].

Security. The three components of the information security CIA triad—confidentiality, integrity and availability—are often used to analyze IoT security issues. Furthermore, secure IoT development guidelines have been released by various governments and organizations as recommendations on how to put in place the necessary security mechanisms, such as the already mentioned ENISA [3] and GSMA [7] documents; to them we add, for example, the IoT device cybersecurity requirement catalogs of NIST in the U.S. [16]. Verification of the security component of trustworthiness spans a broad range of methods, from simply asserting that development guidelines have been followed to actual source code analysis.

Privacy. Privacy analysis usually focuses on the data that is gathered by an IoT system (e.g., via sensors), and on how this data is communicated and stored (e.g., in the cloud). The goal of this analysis is to confirm the compliance with appropriate regulations, such as the General Data Protection Regulation (GDPR) in the EU [2], or the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. [20] for health-related applications. In practice, verification of the privacy component of trustworthiness can be done by evaluating the system design, but also after the system is implemented, for instance via network data analysis, etc.

Reliability. Reliability theory is a well-established field, and reliability metrics—such as the mean time to failure (MTTF), or mean time between failures (MTBF)—are widely used, in particular for hardware components that can malfunction as the result of a component or material failure [18]. For IoT and CPS systems, however, software reliability also needs to be taken into account. It is also important to note that for trustworthiness assessment purposes reliability parameters should be specified with statistical confidence intervals, so as to be able to establish a connection with assurance.

Resilience. Resilience is a highly context-dependent property, as it depends on the system architecture, its operational environment, and the nature of the disruptive event [19]. Redundancy is often used in order to enhance a system's resilience, but in order for this to work effectively it must be coupled with the elimination of single points of failure and good maintenance [14]. Graceful degradation is particularly important from a resilience perspective in order to ensure that an IoT system does not misbehave in a manner that can cause risks related to the other components of trustworthiness, such as safety, security or privacy.

3 TRUSTWORTHINESS ASSURANCE METHODOLOGY

We define *trustworthiness assurance* as the measure of the confidence regarding the trustworthiness claims made about a system, and in practice we employ it to refer to the processes used to justify that the system will perform as expected in the face of environmental disturbances, human errors, system faults and attacks, as stated in the trustworthiness definition.

In order to quantify the trustworthiness assurance, we will use the concept of *assurance levels*, which has already been used in the areas of identity proofing—via Identity Assurance Levels (IALs) [4]—and authentication—via Authentication Assurance Levels (AALs) [5, 12]. We consider that the same concept can be applied to trustworthiness, and, by following an approach inspired by that presented in [12], we introduce the use of *Trustworthiness Assurance Levels* (TALs) for quantifying trustworthiness assurance.

In what follows we define the three TALs that we propose, as well as the characteristic criteria for each of them:

- **TAL1**: TAL1 provides some confidence that the system is trustworthy, with each trustworthiness component being verified qualitatively by conducting a checklist verification using technical specifications and self-assessments to ensure that the system meets the corresponding requirements.
- **TAL2**: TAL2 provides high confidence that the system is trustworthy, with each trustworthiness component being verified quantitatively via experimental methods to ensure that the system meets the corresponding requirements.
- **TAL3**: TAL3 provides very high confidence that the system is trustworthy, with each trustworthiness component being verified via both formal and experimental methods to ensure that the system meets the corresponding requirements.

In Table 1 we provide a summary of the key aspects regarding the assessment methods for each trustworthiness component depending on the target TAL. It should be noted that for a given system it is possible to ensure different TALs for different trustworthiness components, having for example the highest TAL for security, privacy and reliability, and lower TALs for safety and resilience, as long as all concerned parties agree with this approach. Such a compromise may be needed especially when it is difficult to fully verify formally and experimentally one aspect, e.g., the overall safety of a system of systems (SoS). In general, however, even complex system evaluation is possible if conducted in a hierarchical manner.

Case Study. To illustrate the applicability of the methodology, we shall discuss a case study that focuses on an actuation application, one of the main ways in which IoT systems are used. In particular, we will analyze a motorized window application (see Fig. 1). The core of the motorized window system is an actuator IoT device. The other system components are: the window to be actuated, the network infrastructure used for communication (wireless router/access point), a controller such as a smart phone that can be used to control the window, and the public cloud that mediates the communication between the smart phone and the IoT device.

This system requires different trustworthiness levels depending on what context it is used in. If we consider that it is used in a smart home, for example, then trustworthiness does not need to be very high, hence the target assurance level could be TAL1 or TAL2—for instance, TAL1 if the window is too small to allow an intruder to enter the home, and TAL2 if the window is bigger. However, if the motorized window is used in a critical infrastructure facility, the target level should be TAL3. As a side note, it can be said that

Table 1: Trustworthiness Assurance Assessment Methods per Component Depending on the Target Assurance Level

Component	TAL	Assessment Methods
Safety	TAL1	Checklist regarding minimum local safety regulations
	TAL2	Experimental verification regarding local safety regulations
	TAL3	Formal and experimental verification regarding local safety regulations
Security	TAL1	Checklist regarding secure development best practices
	TAL2	Experimental verification regarding security controls
	TAL3	Formal and experimental verification regarding security controls
Privacy	TAL1	Checklist regarding data protection measures
	TAL2	Experimental verification regarding privacy controls
	TAL3	Formal and experimental verification regarding privacy controls
Reliability	TAL1	Checklist regarding reliability metrics compared to requirements
	TAL2	Experimental verification regarding reliability metrics
	TAL3	Formal and experimental verification regarding reliability metrics
Resilience	TAL1	Checklist regarding resilience features compared to requirements
	TAL2	Experimental verification regarding resilience features
	TAL3	Formal and experimental verification regarding resilience features

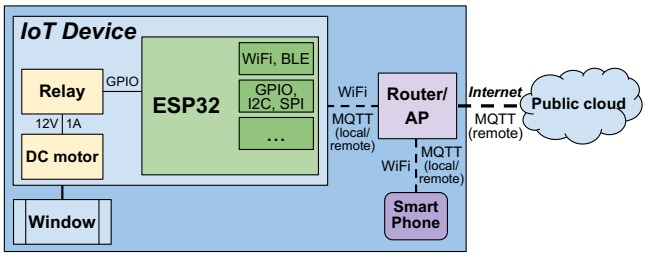

Figure 1: Motorized window actuation system.

for actuation applications, in general, the target TAL depends on the possible harm that the actuated motion can cause, e.g., with higher trustworthiness levels required for an industrial robotic arm operating near factory workers versus that of a toy robot.

Further analysis is needed to establish and validate the processes that should be put in place in order to make possible assessing each of the three trustworthiness assurance levels in practice.

4 CONCLUSION

In this paper we provided an IoT system perspective on trustworthiness and its components—safety, security, privacy, reliability and resilience—emphasizing the many challenges that exist in regard with the assessment and assurance of trustworthiness.

We also defined a methodology based on trustworthiness assurance levels for quantifying the measure of the confidence one can have in the claims made about the trustworthiness of an IoT system. The proposed methodology extends the scope of the trustworthiness analysis from the typical security assurance to encompass all the five components of trustworthiness. A motorized window case study was used to show the methodology application in practice.

We are currently working on the implementation of this methodology in the form of a *trustworthiness assurance framework* that will thoroughly cover both the formal and experimental aspects of trustworthiness verification, and that will provide detailed controls for each trustworthiness component.

REFERENCES

[1] Claude Baudoin, Erin Bournival, Marcellus Buchheit, and Ruben Guerrero. 2020. The Industrial Internet of Things Vocabulary. Industrial Internet Consortium.
[2] European Parliament and Council of the European Union. 2016. General Data Protection Regulation (GDPR) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[3] European Union Agency for Cybersecurity (ENISA). 2019. Good Practices for Security of IoT – Secure Software Development Lifecycle.
[4] Paul Grassi, James Fenton, Naomi Lefkovitz, Jamie Danker, Yee-Yin Choong, Kristen Greene, and Mary Theofanos. 2017. Digital Identity Guidelines: Enrollment and Identity Proofing. Special Publication (NIST SP) - 800-63A, National Institute of Standards and Technology.
[5] Paul Grassi, Elaine Newton, James Fenton, Ray Perlner, Andrew Regenscheid, William Burr, Justin Richer, Naomi Lefkovitz, Jamie Danker, Yee-Yin Choong, Kristen Greene, and Mary Theofanos. 2017. Digital Identity Guidelines: Authentication and Lifecycle Management. Special Publication (NIST SP) - 800-63B, National Institute of Standards and Technology.
[6] Edward Griffor, Christopher Greer, David Wollman, and Martin Burns. 2017. Framework for Cyber-Physical Systems: Volume 1, Overview. Special Publication (NIST SP) - 1500-201, National Institute of Standards and Technology.
[7] GSM Association (GSMA). 2020. GSMA IoT Security Guidelines and Assessment.
[8] Industrial Internet Consortium (IIC). 2022. Industrial Internet Consortium web page. https://www.iiconsortium.org/.
[9] International Organization for Standardization. 2018. Road vehicles – Functional safety. ISO 26262:2018.
[10] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). 2021. Internet of Things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes. ISO/IEC 30147:2021.
[11] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). 2021. ISO/IEC JTC 1/SC 41: Internet of things and digital twin. https://www.iso.org/committee/6483279.html.
[12] International Telecommunication Union. 2020. Entity authentication assurance framework. ITU-T Recommendation X.1254.
[13] Japan Automobile Manufacturers Association (JAMA). 2020. Self-driving safety assessment framework (in Japanese). https://www.jama.or.jp/safe/automated_driving/pdf/framework.pdf.
[14] Gary Marshall and David Chapman. 2002. Resilience, Reliability and Redundancy. http://copperalliance.org.uk/uploads/2018/03/41-resilience-reliability-and-redundancy.pdf.
[15] Katerina Megas, Barbara Cuthill, and Sarbari Gupta. 2021. Establishing Confidence in IoT Device Security: How do we get there? National Institute of Standards and Technology, white paper (draft).
[16] National Institute of Standards and Technology (NIST). 2021. IoT Device Cybersecurity Requirement Catalogs. https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/.
[17] National Institute of Standards and Technology (NIST). 2022. NIST Cybersecurity for IoT Program web page. https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.
[18] Marvin Rausand, Anne Barros, and Arnljot Hoyland. 2020. *System Reliability Theory: Models, Statistical Methods, and Applications* (3 ed.). John Wiley & Sons, New York, NY, USA.
[19] Payuna Uday and Karen Marais. 2015. Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges. *Systems Engineering* 18, 5 (2015), 491–510.
[20] U.S. Department of Health & Human Services. 1996. Health Insurance Portability and Accountability Act (HIPAA). https://www.hhs.gov/hipaa/index.html.