A Proposal to Apply a Risk Assessment Methodology for IoT Systems to a Smart Childhood Obesity Caring Solution

Sergio Luis Ribeiro[a], Emilio Nakamura[a], Rodrigo Lima Verde Leal[a]

a) Fundação Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPqD, Campinas, SP, Brazil

ABSTRACT

This paper presents a risk assessment methodology focused on privacy, security, safety, resilience and reliability to IoT systems. The methodology is composed of ten phases that comprehends the risks elements to calculate the probability of a threat agent to explore one or more vulnerabilities in an IoT asset that turns a threat into an incident that causes impacts on different actors: manufacturers, developers, customers, integrators, service providers and users.

KEY WORDS:

Risk, privacy, security, safety, methodology, IoT.

INTRODUCTION

IoT systems require different security levels depending on their specific use case. Attacks in any of their assets may cause global impacts. The proposed risk assessment methodology takes the use case point of view for the IoT system to provide an integrated security view that directs the actions to be taken by the different actors. For instance, sensors or actuators manufacturers and IoT platform or applications developers can implement the necessary security controls highlighted by that specific use case. Integrators and service providers can build an IoT system using only the assets that comply with the necessary security levels. In addition, users can choose the best IoT system based on the provided security requirements.

IoT systems have key objectives regarding trustworthiness [1]: privacy, security, safety, reliability and resilience. The proposed methodology focuses on these objectives to calculate an IoT system risks. It is desirable that this methodology is applied to a smart childhood obesity caring solution being developed in project OCARIoT.

RISK ASSESSMENT METHODOLOGY

Proper risk assessment considers the probability of a threat agent exploring a vulnerability in an asset, turning a threat into an incident that represents an impact. The starting point of the methodology is to consider that it is not possible to protect against unknown or mistakenly assessed risks. As a part of risk management processes (ISO 31000:2018 [2]), risk assessment provides guidance to define and implement security controls that are both efficient and effective. The limited available resources are used to treat the most important risks in an organized and formal way, without politics, personal preferences or interferences.

Risk assessment can be performed in different contexts, according to the desired risk view and the involved actors. In IoT, there are views for sensors and actuators manufacturers, for platform, application and developers, for customers (home, health, city, industry), or for integrators, service providers and for users. The proposed methodology [3] has 10 phases (Figure 1) and defines the use case as the context for the risk assessment for all the actors. The main reason is the multiplied cyber-physical attack points resulting from integration between sensors, actuators, platforms, applications and users where an attack in one point affects the whole system. The other reason is that a same asset can be used in different IoT contexts that require different security levels based on the specific risks involved.

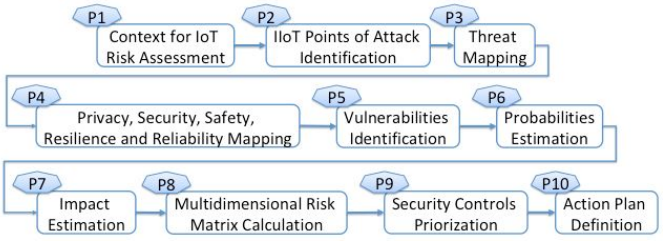

Figure 1: 10-phase methodology.

PROJECT OCARIOT

The main objective of OCARIoT is to provide an IoT-based personalised coaching solution guiding children to adopt healthy eating and physical activity behaviour. The IoT network will allow us to observe child activity patterns of daily living, health evolution, physiological & behavioural parameters and environmental data. All this information combined with medical patterns will allows us to provide a customised obesity coaching plan while enabling children to remain active and engaged in their well-being and healthy habits management. OCARIoT will demonstrate and validate its results on three specific pilot sites in Spain, Greece and Brazil.

PRELIMINARY RESULTS

The project is still in its early stages. Since OCARIoT can generate, manipulate and store personal information, it is desirable, under the project's activities, to carry out a risk assessment throughout the Pilot's environment, in order to determine whether the proposed controls and best practices have been followed. Each of the abovementioned phases will by undertaken, considering the involved actors (children, educators and families) and scenarios (@school, @home and @city).

ACKNOWLEDGEMENT

The authors acknowledge the financial support given to this work, under project OCARIoT, which received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731533 and the RNP under No 3007. This paper reflects only the author's views and the Agencies are not responsible for any use that may be made of the information contained therein.

REFERENCES

[1] Industrial Internet Consortium, "Industrial Internet of Things Volume G4: Security Framework", IIC:PUB:G4:V1.0:PB:20160926, September, 2016, http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf. Accessed in Feb 1, 2018.

[2] International Organization for Standardization, "ISO 31000:2018, Risk management – Guidelines", 2018.

[3] Nakamura, Emilio; Ribeiro, Sergio. "A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems". Global IoT Summit Proceedings. 2018.