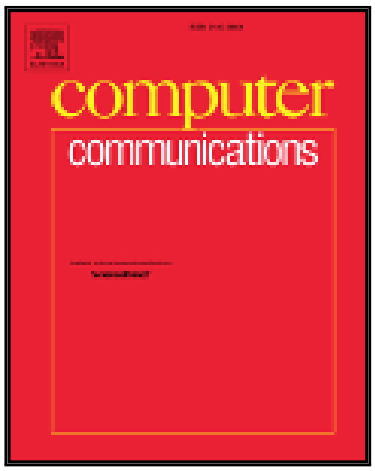

A Risk Assessment Methodology for the Internet of Things

Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi,
Alberto Coen-Porisini

PII: S0140-3664(18)30348-7
DOI: 10.1016/j.comcom.2018.07.024
Reference: COMCOM 5743

To appear in: *Computer Communications*

Received date: 10 April 2018
Revised date: 29 June 2018
Accepted date: 20 July 2018

Please cite this article as: Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini, A Risk Assessment Methodology for the Internet of Things, *Computer Communications* (2018), doi: 10.1016/j.comcom.2018.07.024

A Risk Assessment Methodology for the Internet of Things

Sabrina Sicari*‡, Alessandra Rizzardi*, Daniele Miorandi§, Alberto Coen-Porisini*
*Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria,
via Mazzini 5 - 21100 Varese (Italy)
§U-Hopper, via R. da Sanseverino 95, 38121 Trento, Italy
‡Corresponding author
Email: {sabrina.sicari; alessandra.rizzardi; alberto.coenporisini}@uninsubria.it,
daniele.miorandi@u-hopper.com

***Abstract*—Letting both data producers and data consumers be aware of the levels of security and privacy guaranteed within an IoT-based system represents an important goal to be pursued. In fact, the presence of multiple and heterogeneous data sources, as well as wireless communication standards, increases the risk of violation in IoT scenarios. Besides controlling the behavior of data sources and regulating the access to resources by the interested parties, it is also fundamental to investigate how trustworthy is the platform that manages the provided information and services. To this end, risk assessment techniques can be adopted, with the aim of evaluating the reliability and the robustness towards malicious attacks of the components belonging to the IoT platform. In this paper, a general-purpose methodology for assessing the risk is proposed to be applied to end-to-end systems. More in detail, the proposed approach takes into account both static and dynamic features/components of an IoT system in an *objective* manner, following the whole data life cycle. Such an aspect represents the main advantage of the presented solution, which is concretely demonstrated within the real prototype implementation of an existing IoT middleware, in order to prove its feasibility.**

I. Introduction

Nowadays, most of our every-day and business activities depend on computer-based systems, which are even more moving towards mobile applications. Such an evolution is encouraged by the diffusion of Internet platforms that allow to be connected everywhere in the world. In this scenario, Internet of Things (IoT) technology has emerged thanks to the availability of "smart" devices. They are able to embed wireless sensors, actuators, RFID, NFC, and other similar technologies, which allows such devices to acquire information from the surrounding environment. In this way, it becomes easier the transmission of a huge amount of heterogeneous data that can be used with the final aim of providing customized services to the interested users. This is, in few words, the revolution carried out by the IoT paradigm [1].

Obviously, in order to deal with such a huge amount of information, a scalable platform has to be designed and put in act. It should be able to gather data from heterogeneous sources, process and structuring the data chunks in a uniform representation, and, finally, share them in the form of innovative and useful services. Hence, the IoT platform must be able to manage the whole data life cycle in each specific context.

Note that, to encourage the spreading of IoT applications, end-users (i.e., mainly data consumers) should trust the IoT system that manages both their information and data gathered from unknown sources, expecting that it will provide services with a degree of confidentiality, integrity, availability, and privacy compatible with their needs. Unfortunately, IoT platforms, in general, actually guarantee neither proper security violation controls nor a well-defined assessment of the risk to which the system could be exposed. Users typically know only the interface of the system, but have a little knowledge of how their information are treated, processed and shared. Such aspects are also important for software developers who design and implement the functionalities for the IoT platform itself. Therefore, it is fundamental to carry out a risk evaluation, with three final goals:

- Assessing how much users should believe in the system trustworthiness
- Revealing weaknesses of the existing platforms
- Evaluating possible countermeasures or improvements of the actual system components, in order to make the platform more resilient towards malicious attacks.

To cope with such issues, in this paper, we present a risk analysis methodology, targeted to end-to-end systems, since it comprehensively considers the whole data life cycle of an IoT platform. The proposed approach takes into account both static and dynamic features/components of an IoT system and aims to reveal the existing