

Accepted Manuscript

Modelling Trust Dynamics in the Internet of Things

Carmen Fernandez-Gago, Francisco Moyano, Javier Lopez

PII: S0020-0255(17)30536-4
DOI: [10.1016/j.ins.2017.02.039](https://doi.org/10.1016/j.ins.2017.02.039)
Reference: INS 12762

To appear in: *Information Sciences*

Received date: 16 November 2015
Revised date: 1 December 2016
Accepted date: 15 February 2017

Please cite this article as: Carmen Fernandez-Gago, Francisco Moyano, Javier Lopez, Modelling Trust Dynamics in the Internet of Things, *Information Sciences* (2017), doi: [10.1016/j.ins.2017.02.039](https://doi.org/10.1016/j.ins.2017.02.039)



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Modelling Trust Dynamics in the Internet of Things

Carmen Fernandez-Gago^a, Francisco Moyano^a, Javier Lopez^a

^a*Network, Information and Computer Security Lab
University of Malaga, 29071 Malaga, Spain*

Abstract

The Internet of Things (IoT) is a paradigm based on the interconnection of everyday objects. It is expected that the ‘things’ involved in the IoT paradigm will have to interact with each other, often in uncertain conditions. It is therefore of paramount importance for the success of IoT that there are mechanisms in place that help overcome the lack of certainty. Trust can help achieve this goal. In this paper, we introduce a framework that assists developers in including trust in IoT scenarios. This framework takes into account trust, privacy and identity requirements as well as other functional requirements derived from IoT scenarios to provide the different services that allow the inclusion of trust in the IoT.

Keywords: Trust, Internet of Things, Dynamic framework

1. Introduction

The Internet of Things (IoT) is a paradigm based on the interconnection of everyday objects. According to the Gartner report for 2013 [3], 26 billion objects are expected to be connected in the IoT by 2020. From an economic perspective, the same report also highlights that IoT is expected to generate \$1.9 trillion from the production of IoT products and service suppliers, which will translate into economic growth and employment. At the same time the amount of data managed in the IoT makes it necessary to look at the data-centric perspective [24] and consider the privacy implications that this might raise. The advantages brought by IoT could be seriously threatened if the reception from society is negative. This could be a possibility if citizens, companies and administrations feel that they cannot trust the IoT. Users are becoming more aware of the importance of protecting their private information [2, 14], and companies are increasingly realising that an incorrect security strategy can lead to important economic and reputation losses, and eventually, to bankruptcy¹.

Email addresses: mcgago@lcc.uma.es (Carmen Fernandez-Gago), moyano@lcc.uma.es (Francisco Moyano), jlm@lcc.uma.es (Javier Lopez)

¹<http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html>

Download English Version:

<https://daneshyari.com/en/article/4944540>

Download Persian Version:

<https://daneshyari.com/article/4944540>

[Daneshyari.com](https://daneshyari.com)