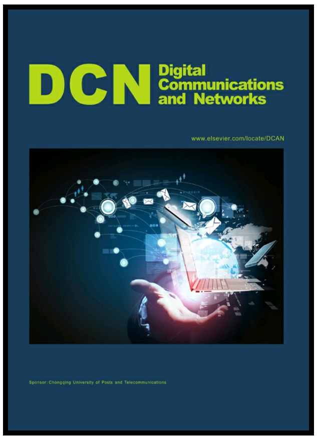
DCN
Digital Communications and Networks
www.elsevier.com/locate/DCAN
Sponsor: Chongqing University of Posts and Telecommunications

www.elsevier.com/locate/dcan

A Roadmap for Security Challenges in Internet of Things

Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou

PII: S2352-8648(17)30021-4
DOI: http://dx.doi.org/10.1016/j.dcan.2017.04.003
Reference: DCAN81

To appear in: *Digital Communications and Networks*

Cite this article as: Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal and Ziec Chtourou, A Roadmap for Security Challenges in Internet of Things, *Digitc Communications and Networks,* http://dx.doi.org/10.1016/j.dcan.2017.04.003

Digital Communications and Networks(DCN)

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/dcan

A Roadmap for Security Challenges in Internet of Things

Arbia Riahi Sfar[ab], **Enrico Natalizio**[b], **Yacine Challal**[c], **Zied Chtourou**[a]

[a]**VRIT Lab - Military Academy, Nabeul, Tunisia**
[b]**Sorbonne universites, Universite de technologie de Compiegne, CNRS, Heudiasyc UMR 7253, CS 60319 ; 60203 Compiegne Cedex, France**
[c]**Laboratoire de Methodes de Conception de Systemes (LMCS), Ecole Nationale Superieure d'Informatique (ESI), Centre de Recherche sur l'Information Scientifique et Technique (CERIST) Algiers, Algeria**

Abstract

Unquestionably, communicating entities (*objects*, or *things*) in the Internet of Things (IoT) context, are acquiring an active role in human activities, systems and processes. The high connectivity of intelligent objects and their severe constraints lead to many security challenges, which are not included into the classical formulation of security problems and solutions. "Security Shield for Internet of Things" has been identified by DARPA (Defense Advanced Research Projects Agency) as one of the four projects with a potential broader impact larger than the Internet itself [1]. To help interested researchers to contribute to this research area, an IoT security roadmap overview is presented in this work based on a novel cognitive and systemic approach. The role of each component of the approach will be explained and interactions with the other main components of the proposed scheme and their impact on the overall system will be detailed. A case study will be presented to highlight components and interactions of the systemic and cognitive approach. Then, security questions about privacy, trust, identification and access control will be discussed. According to the novel taxonomy of IoT framework, different research challenges will be highlighted, important solutions and research activities will be exposed, and interesting research directions will be proposed. In addition, current standardization activities will be surveyed and discussed to ensure security of IoT components and applications.

KEYWORDS:
Internet of Things, Systemic and cognitive approach, Security, Privacy, Trust, Identification, Access Control.

1. Introduction

The long history of the Internet started in the 1950s following the development of electronic computers. Packet switched networks as the ARPANet were developed in the 1960s and the 1970s by using a variety of protocols to join together separate networks. In the 1980s, the Internet protocol suite (TCP/IP) was standardized, and the concept of the Internet as a world wide network was introduced. In the 1990s, thanks to the introduction of almost instantaneous communications, the Internet has led to a real revolution of everyday life domains shown in a wide variety of popular networked applications.

The concept of the Internet of Things (IoT) was introduced in 1999 [1], after the explosion of the wireless devices market, and the introduction of the Radio Frequency Identification (RFID) and the Wireless Sensor Networks (WSN) technologies. IoT concept aims at connecting anything, anyone, at anytime in anyplace. It involves things or objects such as sensors, actuators, RFID tags and readers, to permit interaction between the physical and virtual worlds. An illustrative example of IoT application in a smart factory is shown in figure 1. In this system, we can distinguish four main components: person, process, technological ecosystem and intelligent objects. Defi-